

Task Order Request (TOR)
IT Support Services

In support of:

Department of Commerce (DOC)
Office of the Chief Information Officer (OCIO)
Office of IT Services (OITS)

Issued to:

All contractors under the Alliant Small Business
Government wide Acquisition Contract

Issued by

General Services Administration

National Capital Region,
Assisted Acquisition Services
301 7th Street, S.W.
Washington DC, 20407

April 10, 2017

NCR Project: ID11160043

Amendment 0001

SECTION B – SUPPLIES AND SERVICES AND PRICES/COSTS

B.1 GENERAL DESCRIPTION

The contractor shall perform the effort required by this TO on a Firm Fixed Price (FFP), Labor Hour (LH), and Cost Reimbursement basis. The work shall be performed in accordance with all Sections of this Task Order (TO) and the contractor's Basic Alliant Small Business Contract, under which the resulting TO will be placed.

B.2 CONTRACT ACCESS FEE

The General Services Administration's (GSA) operating costs associated with the management and administration of this contract are recovered through a Contract Access Fee (CAF). The amount of the CAF is ¾ % (i.e., (.0075)) of the total price/cost of contractor performance. This TO shall have a separate Contract Line Item Number (CLIN) to cover this access fee, and this CAF shall be obligated at TO award. The CAF is capped at \$100,000 per year.

B.3 ORDER PRICING

The following abbreviations are used in this price tables:

CLIN	Contract Line Item Number
FFP	Firm Fixed Price
LH	Labor Hour
ODC	Other Direct Costs
NTE	Not to Exceed

B.3.1 BASE PERIOD

FFP CLINs

<u>CLIN</u>	Description	QTY	Unit	Unit Price	Total Firm Fixed Price
0001	Task 1 – Transition – In	1	MONTH	\$	\$
0002	Task 2 – Program/Project Management	7	MONTH	\$	\$
0003	Task 3 – Network Operations Support	7	MONTH	\$	\$
0004	Task 4 – Security Operations Support	7	MONTH	\$	\$
0005	Task 5 – System Administration Support	7	MONTH	\$	\$

0006	Task 6 – IT Service Desk Support	4	MONTH	\$	\$
0007	Task 7 – Server Virtualization Support	7	MONTH	\$	\$
0008	Task 8 – HSPD-12 Personal Identification and Verification (PIV) Support	7	MONTH	\$	\$
0012	Task 12 – Audio Visual, and VTC O & M support	5	MONTH	\$	\$

OPTIONAL LABOR HOUR CLINs

CLIN	Description	Maximum Number of Hours	Labor Rate	NTE Ceiling
0009	Task 9 – Building Renovation Support	640	\$	\$
0010	Task 10 – Cloud Migration Support	2,560	\$	\$
0011	Task 11 - New Technical Architecture and Technologies Implementation	2,560	\$	\$
0013	Task 13 – Live Webcast Streaming Support		\$	\$45,000.00

COST REIMBURSEMENT TRAVEL, TOOLS and ODC CLINs

CLIN	Description		Total Ceiling Price
0014	ODCs – Tools/Equipment/Materials Including Indirect Handling Rate____%	NTE	\$1,157,354.00
0015	Long-Distance Travel Including Indirect Handling Rate _____%	NTE	\$15,000.00
0016	Contract Access Fee	NTE	\$

SECTION B – SUPPLIES AND SERVICES AND PRICES/COSTS

TOTAL FFP CLINs (CLINs 0001-0008, 0012) \$ _____

TOTAL OPTIONAL LH CLINs (0009-0011, 0013) \$ _____

TOTAL BASE PERIOD: \$ _____

B.3.2 FIRST OPTION PERIOD

FFP CLINs

<u>CLIN</u>	Description	QTY	Unit	Unit Price	Total Firm Fixed Price
1001	Task 2 – Program/Project Management	12	MONTH	\$	\$
1002	Task 3 – Network Operations Support	12	MONTH	\$	\$
1003	Task 4 – Security Operations Support	12	MONTH	\$	\$
1004	Task 5 – System Administration Support	12	MONTH	\$	\$
1005	Task 6 – IT Service Desk Support	12	MONTH	\$	\$
1006	Task 7 – Server Virtualization Support	12	MONTH	\$	\$
1007	Task 8 – HSPD-12 Personal Identification and Verification (PIV) Support	12	MONTH	\$	\$
1011	Task 12 – Audio Visual, and VTC O & M support	12	MONTH	\$	\$

SECTION B – SUPPLIES AND SERVICES AND PRICES/COSTS

OPTIONAL LABOR HOUR CLINs

CLIN	Description	Maximum Number of Hours	Labor Rate	NTE Ceiling
1008	Task 9 – Building Renovation Support	3,840	\$	\$
1009	Task 10 – Cloud Migration Support	7,680	\$	\$
1010	Task 11 - New Technical Architecture and Technologies Implementation	7,680	\$	\$
1012	Task 13 – Live Webcast Streaming Support		\$	\$45,000.00

COST REIMBURSEMENT TRAVEL, TOOLS and ODC CLINs

CLIN	Description		Total Ceiling Price
1013	ODCs – Tools/Equipment/Materials Including Indirect Handling Rate____%	NTE	\$1,157,354.00
1014	Long-Distance Travel Including Indirect Handling Rate _____%	NTE	\$15,000.00
1015	Contract Access Fee	NTE	\$

TOTAL FFP CLINs (CLINs 1001-1007, 1011) \$ _____

TOTAL OPTIONAL LH CLINs (1008-1010, 1012) \$ _____

TOTAL OPTION PERIOD ONE: \$ _____

B.3.3 SECOND OPTION PERIOD

FFP CLINs

SECTION B – SUPPLIES AND SERVICES AND PRICES/COSTS

<u>CLIN</u>	Description	QTY	Unit	Unit Price	Total Firm Fixed Price
2001	Task 2 – Program/Project Management	12	MONTH	\$	\$
2002	Task 3 – Network Operations Support	12	MONTH	\$	\$
2003	Task 4 – Security Operations Support	12	MONTH	\$	\$
2004	Task 5 – System Administration Support	12	MONTH	\$	\$
2005	Task 6 – IT Service Desk Support	12	MONTH	\$	\$
2006	Task 7 – Server Virtualization Support	12	MONTH	\$	\$
2007	Task 8 – HSPD-12 Personal Identification and Verification (PIV) Support	12	MONTH	\$	\$
2011	Task 12 – Audio Visual, and VTC O & M support	12	MONTH	\$	\$

OPTIONAL LABOR HOUR CLINs

CLIN	Description	Maximum Number of Hours	Labor Rate	NTE Ceiling
2008	Task 9 – Building Renovation Support	3,840	\$	\$
2009	Task 10 – Cloud Migration Support	7,680	\$	\$
2010	Task 11 - New Technical Architecture and Technologies Implementation	7,680	\$	\$
2012	Task 13 – Live Webcast Streaming Support		\$	\$45,000.00

SECTION B – SUPPLIES AND SERVICES AND PRICES/COSTS

COST REIMBURSEMENT TRAVEL, TOOLS and ODC CLINs

CLIN	Description		Total Ceiling Price
2013	ODCs – Tools/Equipment/Materials Including Indirect Handling Rate____%	NTE	\$1,900,000.00
2014	Long-Distance Travel Including Indirect Handling Rate _____%	NTE	\$15,000.00
2015	Contract Access Fee	NTE	\$

TOTAL FFP CLINs (CLINs 2001-2007, 2011) \$ _____

TOTAL OPTIONAL LH CLINs (2008-2010, 2012) \$ _____

TOTAL OPTION PERIOD TWO: \$ _____

B.3.4 THIRD OPTION PERIOD

FFP CLINs

<u>CLIN</u>	Description	QTY	Unit	Unit Price	Total Firm Fixed Price
3001	Task 2 – Program/Project Management	12	MONTH	\$	\$
3002	Task 3 – Network Operations Support	12	MONTH	\$	\$
3003	Task 4 – Security Operations Support	12	MONTH	\$	\$
3004	Task 5 – System Administration Support	12	MONTH	\$	\$
3005	Task 6 – IT Service Desk Support	12	MONTH	\$	\$
3006	Task 7 – Server Virtualization Support	12	MONTH	\$	\$

3007	Task 8 – HSPD-12 Personal Identification and Verification (PIV) Support	12	MONTH	\$	\$
3011	Task 12 – Audio Visual, and VTC O & M support	12	MONTH	\$	\$

OPTIONAL LABOR HOUR CLINs

CLIN	Description	Maximum Number of Hours	Labor Rate	NTE Ceiling
3008	Task 9 – Building Renovation Support	3,840	\$	\$
3009	Task 10 – Cloud Migration Support	7,680	\$	\$
3010	Task 11 - New Technical Architecture and Technologies Implementation	7,680	\$	\$
3012	Task 13 – Live Webcast Streaming Support		\$	\$45,000.00

COST REIMBURSEMENT TRAVEL, TOOLS and ODC CLINs

CLIN	Description		Total Ceiling Price
3013	ODCs – Tools/Equipment/Materials Including Indirect Handling Rate____%	NTE	\$1,157,354.00
3014	Long-Distance Travel Including Indirect Handling Rate _____%	NTE	\$15,000.00
3015	Contract Access Fee	NTE	\$

TOTAL FFP CLINs (CLINs 3001-3007, 3011) \$ _____

TOTAL OPTIONAL LH CLINs (3008-3010, 3012) \$ _____

TOTAL OPTION PERIOD THREE: \$ _____

SECTION B – SUPPLIES AND SERVICES AND PRICES/COSTS

B.3.5 FOURTH OPTION PERIOD

FFP CLINs

<u>CLIN</u>	Description	QTY	Unit	Unit Price	Total Firm Fixed Price
4001	*Task 1 – Transition - Out	1	MONTH	\$	\$
4002	Task 2 – Program/Project Management	12	MONTH	\$	\$
4003	Task 3 – Network Operations Support	12	MONTH	\$	\$
4004	Task 4 – Security Operations Support	12	MONTH	\$	\$
4005	Task 5 – System Administration Support	12	MONTH	\$	\$
4006	Task 6 – IT Service Desk Support	12	MONTH	\$	\$
4007	Task 7 – Server Virtualization Support	12	MONTH	\$	\$
4008	Task 8 – HSPD-12 Personal Identification and Verification (PIV) Support	12	MONTH	\$	\$
4012	Task 12 – Audio Visual, and VTC O & M support	12	MONTH	\$	\$

* CLIN 4001, the two month transition-out period will only occur once and may occur at the end of any performance period.

SECTION B – SUPPLIES AND SERVICES AND PRICES/COSTS

OPTIONAL LABOR HOUR CLINs

CLIN	Description	Maximum Number of Hours	Labor Rate	NTE Ceiling
4009	Task 9 – Building Renovation Support	3,840	\$	\$
4010	Task 10 – Cloud Migration Support	7,680	\$	\$
4011	Task 11 - New Technical Architecture and Technologies Implementation	7,680	\$	\$
4013	Task 13 – Live Webcast Streaming Support		\$	\$45,000.00

COST REIMBURSEMENT TRAVEL, TOOLS and ODC CLINs

CLIN	Description		Total Ceiling Price
4014	ODCs – Tools/Equipment/Materials Including Indirect Handling Rate ____%	NTE	\$1,157,354.00
4015	Long-Distance Travel Including Indirect Handling Rate _____%	NTE	\$15,000.00
4016	Contract Access Fee	NTE	\$

TOTAL FFP CLINs (CLINs 4001-4008, 4012) \$ _____

TOTAL OPTIONAL LH CLINs (4009-4011, 4013) \$ _____

TOTAL OPTION PERIOD FOUR: \$ _____

GRAND TOTAL ALL CLINs \$ _____

THE NTE CEILING AMOUNT REPRESENTS THE MAXIMUM AMOUNT OF THE GOVERNMENT'S LIABILITY. THE CONTRACTOR EXCEEDS THE CEILING AT ITS OWN RISK.

SECTION B – SUPPLIES AND SERVICES AND PRICES/COSTS

B.4 SECTION B TABLES (CLINs DESCRIPTIONS)

B.5 INDIRECT/MATERIAL HANDLING RATE

Travel and ODCs costs incurred may be burdened with the Contractor's indirect/material handling rate in accordance with the Contractor's basic contract. If no indirect/material handling rate is allowable in accordance with the Contractor's basic contract, no indirect/material handling rate shall be applied to or reimbursed on such costs.

B.6 DIRECT LABOR RATES

Labor categories proposed shall be mapped to existing Alliant Small Business labor categories.

B.7 OPTIONAL SERVICES

These activities will be exercised as needed by DOC and are designated under an optional CLIN. As with all optional CLINs in this solicitation, there is no guarantee that DOC will decide to use these services.

B.8 SURGE LABOR MODIFICATIONS

The Government may modify the task order to address unusual call-center events requiring significant additional personnel. Such modifications are specifically defined to be within the scope of this task order. DOC anticipates this happening 2-3 times per year.

B.9 ON-BOARDING ADDITIONAL STAFF

The Contracting Officer will provide written notice to the Contractor at least 30 calendar days prior to any unilateral exercise of the Optional CLINs. The start date for the support will be mutually agreed upon between both the Government and the Contractor.

SECTION C – DESCRIPTION/SPECIFICATIONS/STATEMENT OF WORK

C.1 PURPOSE

Within the OCIO, the Office of IT Services operates the computer and telecommunications network and security infrastructure at the Herbert C. Hoover building (HCHB). DOC's headquarters is located at 1401 Constitution Avenue, Washington, DC, 20230. The HCHB network infrastructure (HCHBNet) provides data, voice, WiFi/wireless, and emergency broadcast services to several Operating Units that reside within DOC headquarters. Additional services include security monitoring, analysis, and policy enforcement of the network. The Public Address (PA) system support is also provided to the non-renovated sections of the building and is part of this task order. The renovated sections are supported by a fire alarm system supported by GSA via Building Management that is not part of this task order. Voice, data and other IT services are also offered to limited users in the Ronald Reagan Building. The primary purpose of this task order is to provide ongoing operation and maintenance (O&M) of HCHBNet and to enhance the overall service delivery model for the infrastructure.

This task order will also support HCHB renovation. DOC and the GSA Public Building Service are renovating HCHB on a 15 to 20 year schedule. As renovations continue, DOC will require the Contractor to operate, maintain, replace, and upgrade the cable plant, servers, and related HCHBNet components as part of building renovation. This includes supporting cable plant moves, adds and changes (MACs) in the newly renovated spaces as well as cable plant, IT, and phone MACs for work related to office requirements.

In addition, this task order will provide ancillary information technology (IT) support and engineering services for HCHBNet users and applications that run on or over HCHBNet. Additionally, operations and maintenance of network components that extend beyond HCHB, including the internet, MPLS and TLS services; and DOC OCIO and operating units' network, system engineering and system enhancement projects.

Furthermore, this task order will provide service desk support for the DOC/Office of the Secretary and three other OUs, including Economic Development Administration (EDA), Economic and Statistics Administration (ESA) and Minority Business Development Administration (MBDA).

Lastly, this task order will provide Audio Visual and VTC O&M and live webcast streaming support. This includes support to ensure the audio visual and video teleconferencing systems are operating at an optimal level and live webcast events are conducted and supported.

C.1.2 BACKGROUND

The DOC OCIO is responsible for the development and implementation of the agency's Enterprise Architecture, spanning IT systems and technical services across the department's Operating Units (OU) (International Trade Administration, National Telecommunications and Information Administration, Economic Development Administration, etc.) and staff offices (Chief Financial Officer, etc.). In this role, the OCIO is supported by the departments

SECTION C – DESCRIPTION/SPECIFICATIONS/STATEMENT OF WORK

Enterprise Architecture Advisory Group and other stakeholders. Departmental adherence to Government-wide guidelines for IT work that includes security and the system development life cycle (ITSDLC) are also within the OCIO's span of responsibility. The DOC OCIO is responsible for the action plans identified in the Federal CIO's 25 Point Implementation Plan to Reform Federal Information Technology Management include the consolidation of commodity IT spending for strategic sourcing and migration of IT services into the Cloud. This task order will support and implement these initiatives. The HCHBNet infrastructure is the primary focus of this task order. HCHBNet and DOC operating units' interconnected local and wide area networks have a key role in Commerce Enterprise Architecture, IT security, and the department's communications and operations. Other DOC bureaus located at the Herbert C. Hoover Building will leverage this task order for strategic sourcing of network and security operational services.

HCHBNet is a strategically planned, inter-networked, centralized communications infrastructure that provides connectivity for DOC automated information systems operated within the HCHB. It provides the platform for Operating Units to connect their automated information systems to one centralized core backbone in the HCHB. This backbone is logically redundant and fault tolerant and includes multiple layers of security from the external perimeter through to the data or object level of the applications and data resources accessed through the HCHB network infrastructure.

DOC designed HCHBNet as a homogeneous network that allows Operating Units (OUs) located at HCHB to transfer data, voice and video securely, reliably and efficiently. It also provides for consolidation of Operating Unit networks onto a common, standardized, high-speed infrastructure, controlled, maintained and enhanced by a central OCIO entity. DOC designed HCHBNet to evolve and scale to support new technologies and bandwidth requirements, and incorporate emerging products that permit voice, data and video to share a common, structured infrastructure that is fully documented. Technologies such as cloud services, mobility and virtualization have been incorporated into the HCHBNet.

C.1.3 AGENCY MISSION

The Commerce Department has a wide range of responsibilities in the areas of trade, economic development, technology, entrepreneurship and business development, environmental stewardship, and statistical research and analysis. Within the federal government, the Commerce Department is also the principal defender and champion of the digital economy. Data from the Commerce Department touches every American and informs daily business decisions. Commerce data enable start-ups, move markets, protect life and property, and power both small and multi-billion dollar companies. They also have a unique role in carrying out the constitutionally mandated decennial census, which serves as the basis of ensuring America's representative democracy. It determines the allocation of billions in federal dollars to states and the drawing of congressional districts, among other important activities. Within the Commerce Office of the Secretary, the OCIO provides information technology (IT) leadership advancing the mission of the Department of Commerce. It leads the management of information resources,

SECTION C – DESCRIPTION/SPECIFICATIONS/STATEMENT OF WORK

ensuring that Commerce programs and Bureaus provide world-class information services to end users, improving the efficiency of delivering information services, and empowering and equipping a workforce that is highly motivated and customer service oriented. One of OCIO's priorities is to continuously improve secure access to data, information, and systems and to continuously protect those assets from loss or unauthorized access.

C.2 CURRENT ENVIRONMENT

The Contractor shall conform to the DOC network architecture, security, and operating procedure standards and subsequent DOC or other Government regulations, legislative requirements, industry best practices and revisions to these standards. These include:

- Format, function, data, and interface standards of HCHBNet and supporting server infrastructure.
- HCHB System Security Plan. This includes Acquisition Policy as identified in the DOC IT Security Program Policy (ITSPP). The ITSPP provides policy for the DOC and is used as the guiding policy for the HCHBNet which is managed by Office of the Secretary of Commerce (OSEC)/OCIO.
- SOPs - OITS Standard Operating Procedures. SOPs are subject to updates, additions, and deletions over time, and maintenance of these SOPs is the Contractor's responsibility.
- Commerce Enterprise Architecture: Maturity Model; Communications Plan; Configuration Management Plan; and System Development Life Cycle (ITSDLC)
- Commerce IT Security and Privacy: IT Security Program Policy; IT Privacy Policy; Electronic Transmission of Personally Identifiable Information (PII)
- Department of Commerce Scalable Project Management Methodology
- Commerce IT Investment Performance Management Policy

The current network was originally designed in 2005, but has undergone numerous upgrades, particularly within in the past 5 years. A recent replacement of access layer switches servicing approximately 5000 users throughout the HCHB was phase 1 of a 2 phase project to perform an overhaul of the existing HCHB network. The current focus is on phase 2 which consists of upgrading the core network devices that are approaching End-of-Life/End-of-Support. The replacement of core backbone infrastructure devices is needed to improve network performance and reliability of the network to meet the growing demands of high-end user computing through cloud services. The network backbone today provides a network transport for services such as wireless and VoIP to all users residing in the building. The Department has already made significant investments in these areas. Additionally, services dependent on the network backbone include video teleconferencing, cloud applications, and online collaboration. The network is physically and logically redundant and fault-tolerant comprising of access switches connected to dual distribution switches, which then connect to dual core switches. These core switches connect to dual perimeter firewalls, which currently serve as primary (active) and secondary (standby) functions. The firewalls connect to the Internet layer devices, which include multiple layers of security from the external perimeter to the data or object level of the applications and data resources accessed through the HCHB network infrastructure. The HCHBNet network topology and connectivity are comprised of a multi-layered model with three

SECTION C – DESCRIPTION/SPECIFICATIONS/STATEMENT OF WORK

distinct layers: the Core Layer, the Distribution Layer, and the Access Layer. Additionally, a new enterprise wireless solution with network access control has been implemented in the newly renovated areas of the building.

Core Layer

The Core Layer consists of two Cisco intelligent switches. The function of the Core Layer is to move packets as rapidly as possible to one of the five Distribution Blocks. The Core has dual load sharing power supplies and redundant Supervisor Modules for resiliency.

Distribution Layer

The Distribution Layer consists of pairs of Cisco intelligent switches. The combination of a distribution switches pair and the switches connected to them are referred to as the “Distribution Block,” and are used as the building block for the HCHBNet design, providing modularity and scalability. The HCHBNet defines six Distribution Blocks, which are described below. The Distribution Layer switches aggregate the traffic from the Access Layer switches. Each Distribution Layer switch includes Intrusion Detection Systems (IDS), Access Control Lists (ACLs) appropriate to the traffic for the distribution block, and redundant power supplies.

Access Layer

The Access Layer is used to concentrate endpoint devices such as workstations, phones, and printers. The Access Layer devices are currently comprised of Cisco Catalyst switches installed in telecommunications closets (Telco closets) throughout the building. Each Access Layer Switch is provisioned with two or three, and in few switches have four, 48-port 10/100 Fast Ethernet switching modules. Each switch features load-sharing power supplies and dual 1000BaseSX uplinks to the Distribution Layer switches.

The Access Layer switches connect to the Distribution Layer switches via standard IEEE 802.1q Gigabit Ethernet Trunks. The Distribution switches are connected to the Core Layer via Gigabit Ethernet fiber links (1000BaseSX). The distribution switch pair is connected to each other via an 802.1q trunk as well.

At the Distribution Layer switches, a Cisco Intrusion Detection System (IDS) Module is implemented to detect unauthorized activities (with the exception of the Management Distribution Block). The switches also apply appropriate ACLs and activity logging to restrict access to required traffic only. The HCHBNet uses a strict VLAN implementation, to isolate specific bureaus and/or other data types (i.e., VoIP is routed via a specific VoIP-VLAN).

Enterprise Wireless Local Area Network

The wireless enterprise is an integration of Cisco wireless communication devices providing client mobility throughout HCHB Campus. The wireless enterprise design consists of employing Cisco access points (APs) partially throughout HCHB Campus accompanied by two High-Availability pair Wireless LAN Controllers (WLC); one foreign controller supporting the AP population and one anchor controller supporting guest users. There is a Network Control System (NCS)/Prime Infrastructure Management server (Prime), two High-Availability pairs of Mobility Service Engines (MSE), and two Identity Services Engines (ISE) distributed between the

SECTION C – DESCRIPTION/SPECIFICATIONS/STATEMENT OF WORK

primary and secondary datacenters for improved reliability. The WLAN and ISE authentication mechanism policy supports wired and wireless networks for peripheral systems and transport communications. The controllers and access points provide basic layer 2 and 3 connectivity to HCHBNet backbone devices upon successful authentication. For enhanced security, various client SSIDs have been implemented for guest vs. HCHB employees. The internal WLANs are non-broadcast SSIDs thus enhancing the security posture of their networks. The DOC Guest WLANs are openly broadcast reflecting the requirement for those networks to be easily accessible. Currently, there are 557 access points installed in the HCHB campus, providing wireless coverage for approximately one third of the campus. Depending on availability of budget, the intent is to have wireless coverage throughout the campus.

Network Backbone Upgrade

The existing network backbone is currently being upgraded from 1Gbps at the access, distribution and core layers. As part of the network refresh, primary and secondary uplinks between the core and distribution switches shall be converted to 10Gbps.

Existing equipment is installed in various telecommunications closets (Telco closets) throughout the campus as well as the primary and secondary data centers also located in the building.

IT Service Desk Support

The OCIO office contracts out for IT support and administration of a fully functional service desk support service for Tier 0, Tier 1, and Tier 2 services. OCIO's management and technical personnel, made up of both federal employees and contractor personnel, form the Office of IT Services (OITS). IT Service Desk (ITSD) provides support to hardware, software, and systems used to collect, process, store, transmit and disseminate data and information. This includes personal computers (desktops and laptops); hand-held computing devices; phones; tablets; printers; scanners; multi-function devices; VoIP phone system; and other peripheral IT equipment. Requirements may also involve the planning and delivery of customer support services, including but not limited to information gathering, installation and configuration of hardware and software, and assistance in response to customer service requests and troubleshooting. Tier 3 services are provided by the Systems Administration, Network Operations Center (NOC) and Security Operations Center (SOC).

OITS provides Information Technology (IT) support to the Office of the Secretary, EDA, ESA and MBDA users, which are primarily located in the HCHB. Outside the HCHB, EDA has six remote offices with approximately 120 employees that are supported through the HCHB service desk.

C.3 SCOPE

The scope of this Task Order includes the following:

- The Contractor shall provide IT service desk support services for the DOC/Office of the Secretary and three other OUs, including Economic Development Administration (EDA), Economic and Statistics Administration (ESA) and Minority Business Development Administration (MBDA).

SECTION C – DESCRIPTION/SPECIFICATIONS/STATEMENT OF WORK

- The Contractor shall provide front-line daily operations support and customer service responsibilities for the Office of IT Services. This entails basic ticket response and ensuring proper customer communications requirements are met. As appropriate, the Contractor shall be responsible for monitoring and maintaining existing security toolsets and policies to mitigate security exploits and vulnerabilities. In addition, the Contractor shall keep up with emerging security threats and information to support OCIO in meeting its mission.
- The Contractor shall respond to inquiries and resolve trouble tickets related to services managed for HCHBNet and its interconnections.
- The Contractor shall operate, maintain, and enhance HCHBNet, its interconnections, and their communications traffic. In addition to data, HCHBNet carries VOIP and legacy telephony, public address, emergency broadcast and video communications traffic.
- The Contractor shall implement IT projects that support HCHB Building Renovation, DOC Operating Units, and System Engineering and Enhancement.
- The principal place of performance will be at HCHB. Work at remote sites interconnected with the HCHB and HCHBNet are also within the scope of this task order.
- The Contractor shall provide vulnerability scanning and assessment support for systems supported by the DOC/OCIO.
- The Contractor shall maintain, operate, and engineer security enforcement tools for the HCHB network infrastructure.
- The Contractor shall provide daily monitoring, analysis, and reporting of security events and incidents as required by the DOC Incident Reporting process and procedures.
- The Contractor shall provide systems administration, Personal Identify Verification (PIV) logical access control (LAC), and server virtualization support.
- The Contractor shall provide full end-to-end support to produce, broadcast and archive events for on-demand viewing. To deliver this capability, the contractor shall provide the following services:
 - Full production support of events to include equipment, staff to set-up and break-down equipment and production services
 - On-line registration for event viewing/participation
 - Web-based transmission of recorded and live events
 - Archiving of events for streaming on-demand
 - Detailed analytical and statistical reporting on participation and viewing of broadcasted events.
- The Contractor shall operate, maintain, install, service and repair complex electronic A/V and IT systems and equipment including 70-volt sound systems, low voltage displays, and technical AV test instruments as a part of his/her normal commitment to DOC.

SECTION C – DESCRIPTION/SPECIFICATIONS/STATEMENT OF WORK

C.4 TASKS

The following tasks are in support of this TO and are detailed below:

- Task 1 –Transition In/Out
- Task 2 – Program Management
- Task 3 - Network Operations Support
- Task 4 – Security Operations Support
- Task 5 – Systems Administration Support
- Task 6 – IT Service Desk Support
- Task 7 – Server Virtualization Support
- Task 8 – HSPD-12 Personal Identification and Verification (PIV) Support
- Task 9 – Building Renovation Support (**Optional**)
- Task 10 – Cloud Migration Support (**Optional**)
- Task 11 – New Technical Architecture and Technologies Implementation (**Optional**)
- Task 12 – Audio Visual and VTC O&M Support
- Task 13 – Live Webcast Streaming Support (**Optional**)

The skill mix and the number of labor hours in the table below are provided for estimation purposes only and may be used to provide a better understanding of the current approach to the requirements. Offerors may provide alternative solutions and/or provide alternative labor categories and hours to meet the conditions of the task requirements and deliverables.

Tasks	Suggested Contractor Staffing
Task 1: Transition In/Out	
Task 2: Program Management	1 Full-time (40 hours per week)
Task 3: Network Operations Support	3 Network Engineers (2 Senior and 1 Mid Level) 2 Network Security Engineer (2 Senior Level) 2 VoIP Engineer (1 Senior and 1 Mid Level) 1 VoIP Technician (Mid Level) 3 Cable Technician (2 Senior and 1 Mid) NOTE: All staff full-time (40 hours per week)
Task 4: Security Operations Support	1 Security Engineer (Senior Level) 2 Security Analyst (Mid Level) NOTE: All staff full-time (40 hours per week)
Task 5: Systems Administration Support	1 Systems Engineer (Senior Level) 2 Systems Administrators (Mid-Level) NOTE: All staff full-time (40 hours per week)
Task 6: IT Service Desk Support	1 Technical Project Manager 5 Tier 1 Support (1 Senior, 4 Mid Level) 5 Tier 2 Support (2 Senior, 3 Mid Level) NOTE: All staff full-time (40 hours per week)
Task 7: Server Virtualization Support	1 Systems Engineer (1 Senior Level) NOTE: All staff full-time (40 hours per week)
Task 8: HSPD-12 Personal Identification and Verification (PIV) Support	1 Systems Engineer (Senior Level) NOTE: All staff full-time (40 hours per week)

Task 12: Audio Visual and VTC O&M Support	1 Audio Visual/VTC Specialist NOTE: All staff full-time (40 hours per week)
---	--

C.4.1 TASK 1 TRANSITION

C.4.1.1 TRANSITION-IN

The contractor shall provide transition-in services. The contractor shall complete Transition-In services within thirty (30) calendar days of the task order start date. The contractor shall work professionally with the outgoing contractor to achieve a successful and timely transition. The contractor shall transition all services without interruption or degradation of service levels. The contractor shall verify system and facility access with the Government. The Contractor shall submit a draft transition-in plan at the kickoff meeting. The transition-in plan shall describe the approach to transition tasks and materials from the outgoing Contractor. The offeror's approach shall incorporate the following: The offeror's transition approach, process, and timelines; The offeror's approach to risk management and mitigation and ensuring disruptions are minimized; The offeror's knowledge transfer and training methodology; How the offeror will handle personnel security adjudication; and the offeror's approach to coordination with the outgoing contractor. Additionally, the transition plan shall include an extensive list of questions and issues the Contractor proposes to address with the outgoing Contractor. The contractor shall submit a Final Transition-In Plan in accordance with the deliverable table in Section F. The final transition-in plan must be detailed and include start-up activities that may be required to transition to full operational capability to successfully assume all duties under this task order. The final transition-in plan must include identification of key transition events and objectives with a corresponding completion timeline. During transition in, the contractor shall become familiar with performance requirements and establish the management organization.

C.4.1.2 TRANSITION-OUT

The contractor shall maintain complete documentation that is 100% assessable to the designated Government representatives via a web portal or some other method directed by the Government. The contractor shall overlap with the incoming contractor during the transition out period, work with Government personnel and the incoming contractor to transfer all knowledge, information and documentation for all projects and tasks related to this task order. At all times during the transition-out period, the contractor must exhibit professional conduct and work hand-in-hand with the incoming contractor to provide for a successful transition-out. The contractor shall submit a Draft Transition-Out Plan and a Final Transition-Out Plan in accordance with the deliverable table. The Final Transition-Out Plan must include all pertinent information for a successful transition, to include at a minimum:

- a. Project management processes
- b. Points of contact
- c. Location of technical and project management documentation
- d. Status of ongoing technical initiatives
- e. Appropriate contractor to contractor coordination to ensure a seamless transition
- f. Schedules and milestones
- g. Document operational baseline

SECTION C – DESCRIPTION/SPECIFICATIONS/STATEMENT OF WORK

- h. Actions required of the Government.
- i. Effective communication with the incoming contractor
- j. A final invoice and close-out schedule with the dates and actions to be completed for TO close-out

C.4.2 TASK 2 – PROJECT MANAGEMENT SUPPORT

The Contractor shall provide program management support under this task order. This includes the management and oversight of all activities performed by contractor personnel, including subcontractors, to satisfy the requirements identified in this task order. The Contractor shall identify a Project Management Professional Certified (PMP) Project Manager (PM) by name, who shall provide management, direction, administration, quality assurance, and leadership of the execution of this task order. This position is considered a key personnel position.

- Update and manage project deliverables, risks registry, tasks and work packages, and contractor resources.
- Conduct recurring (weekly or bi weekly) and ad hoc status meeting with DOC shared services and program management team(s). Contractor shall generate and distribute meeting minutes.
- Monitor and track contractor labors hours, materials, and resources.
- Coordinate all aspects of planning and deployment with DOC, IT support contractors, and other government personnel and key stakeholders.

C.4.2.1 SUBTASK 1 - COORDINATE A PROJECT KICKOFF MEETING

The Contractor shall schedule and coordinate a Project Kick-Off Meeting at the location approved by the Government. The meeting will provide an introduction between the Contractor personnel and Government personnel who will be involved with the Task Order. The meeting will provide the opportunity to discuss technical, management, and security issues. At a minimum, the attendees shall include vital contractor personnel, representatives from OCIO and the operating units, other relevant Government personnel, the Contracting Officer and the Contracting Officer's Representative (COR).

The Contractor shall provide the following at the kickoff meeting:

- Transition-In Plan Draft

C.4.2.2 SUBTASK 2 - PREPARE MONTHLY STATUS REPORTS (MSRS)

The Contractor shall develop and provide a Monthly Status Report (MSR) using MS Office Suite applications, by the 10th calendar day of each month for the previous month. The Contractor shall submit MSRs by electronic mail to the COR. The MSR shall include the following:

- Activities during reporting period, by task (Include: On-going activities, new activities, activities completed; progress to date on all above mentioned activities). Start each section with a brief description of the task.
- Problems and corrective actions taken. Also include issues or concerns and proposed resolutions to address them.

SECTION C – DESCRIPTION/SPECIFICATIONS/STATEMENT OF WORK

- Personnel gains, losses and status
- Government actions required
- Schedule (Shows major tasks, milestones, and deliverables; planned and actual start and completion dates for each).
- Summary of trips taken, etc

C4.2.3 SUBTASK 3 - CONVENE TECHNICAL STATUS MEETINGS

The Contractor's Project Manager shall convene weekly and monthly with the GTR and other vital government stakeholders who will be identified after award. The purpose of these meetings is to ensure all stakeholders are informed of project activity and (for the monthly meeting) the status report, provide opportunities to identify other activities and establish priorities, and coordinate resolution of identified problems or opportunities. The Contractor's Project Manager shall provide minutes of the monthly meetings, including attendance, issues discussed, decisions made, and action items assigned, to the GTR within five calendar days following the meeting. Conference calls, are acceptable.

C.4.2.4 SUBTASK 4 - PREPARE A PROJECT MANAGEMENT PLAN (PMP)

The Contractor shall document all support requirements in a PMP. The PMP shall:

- Describe the proposed management approach
- Contain detailed Standard Operating Procedures (SOPs) for all tasks, including updates to existing SOPs. Note: SOPs are standalone attachments to the PMP.
- Include milestones, tasks, and subtasks required in this Task Order
- Provide for an overall Work Breakdown Structure (WBS) and associated responsibilities and partnerships between Government organizations
- Include the Quality Control Plan (QCP)
- Provide and maintain a master schedule for all projects under this task order

The Contractor shall provide the Government with a draft PMP. The Government will comment on the draft PMP. The final PMP shall incorporate Government comments.

C.4.2.5 SUBTASK 5 - UPDATE THE PROJECT MANAGEMENT PLAN (PMP)

The PMP is an evolutionary document that shall be updated at least annually. The Contractor shall work from the latest Government approved version of the PMP to provide updates.

C.4.2.6 SUBTASK 6 - QUALITY CONTROL PLAN (QCP)

The contractor shall provide a draft Quality Control Plan (QCP) as required in Section F. The final QCP shall incorporate the Government's comments. The contractor shall periodically update the QCP, as changes in program processes occur. At minimum, the QCP shall be reviewed and updated once a year.

Within the QCP, the contractor shall identify its approach for providing quality control in meeting the requirements of the TO. The offeror's QCP shall describe its quality control methodology for accomplishing TO performance expectations and objectives. The contractor

SECTION C – DESCRIPTION/SPECIFICATIONS/STATEMENT OF WORK

shall fully discuss its validated processes and procedures that provide high quality performance for each Task Area. The QCP shall describe how the processes integrate with the Government's requirements and not just state that they are certified in a particular quality standard approach.

C.4.3 TASK 3 – NETWORK OPERATIONS SUPPORT

The Contractor shall provide experienced and qualified professional personnel to provide services to include, but not limited to the following:

- Operate and maintain the network hardware, applications and tools that support the Network Operations Center services. This includes telephone services, HCHB network infrastructure operations support and network security management services. This applies to the Operating Units and commercial entities in the HCHB as well as any of their remote sites that have migrated to the HCHB network infrastructure. Service desk tickets referred to the network operations center (NOC), for telephones, or for the public address system and emergency broadcast system (EBS) are also included.
- Replace hardware and software to support the performance measures listed in the service Level agreements (SLAs) (see Section J). The OCIO, based on a business case, must approve any introduction of new hardware or software brands not currently in the HCHB network infrastructure's inventory. Provide an equipment and maintenance refresh schedule. Maintain an inventory of all hardware and software that supports the HCHBNet. Re-architect and implement migration; make appropriate changes to network zones and enclaves. The hardware refresh cycle is currently 3-5 years for servers and 5-7 years for network equipment; hardware and software costs are reimbursable under the ODC CLIN.
- Move, add, and change network hardware and/or software when it is not associated with building renovation. The Contractor shall remove, replace, upgrade, and/or install cable plant, racks, panels, and other infrastructure that is not associated with building renovation. Cable plant and cable moves, adds, and changes associated with office renovation (CD410's) but not HCHB building renovation are within the scope of Task 3. The contractor shall purchase miscellaneous consumables to supply these moves, adds and changes through the ODC CLIN.
- Provide NOC and SOC operations during core business hours, which are 7:00 a.m. – 6:00 p.m. Monday through Friday (except Federal holidays); special weekend/nighttime requirements (e.g., maintenance and upgrades); and emergency after-hours on-call staff support (including contact information) for assistance at all other times. The Contractor shall obtain approval from the GTR and COR for work outside core business hours.
- Conduct real time network monitoring of HCHBNet performance and usage; and provide weekly, monthly and quarterly reports to management on the health, stability, utilization and any changes made to the HCHB network infrastructure.
- Document new and update Standard Operating Procedures (SOPs) as a result of new tools, systems and/or processes.
- Provide integrated, transparent network maintenance, including the cable plant. Document the required maintenance and obtain approval via the Change Control Board process (Section J) prior to conducting the network maintenance.

SECTION C – DESCRIPTION/SPECIFICATIONS/STATEMENT OF WORK

- Receive audible Public Address System emergency broadcast successfully during normal working hours in all HCHB common areas.
- Provide support for existing wireless infrastructure that is connected to the HCHB network infrastructure. Approximately 560 Cisco wireless access points have been deployed in the HCHB campus. Both guest wireless and internal wireless networks need to be managed.
- Log and track all telecommunications and network-related customer service requests from receipt of request to completion of service via the Service Now tracking system in real time. ServiceNow is purchased as a service for the government and operated by the contractor. Monitor email notification of Service Now tickets assigned to the NOC. Respond to Service Now tickets. Update ticket with diagnostic, corrective, referral or other dispositive actions taken. Route to other responding activities when appropriate. Close out assigned trouble tickets when completed.
- Trouble ticket receipt may be by referral from the OCIO IT Service Desk, direct to Contractor's staff, or from other sources. Request may be received from other customers within HCHB as other service desks exist within HCHB. The awarded contractor will maintain the OCIO ITSD.
- Respond to and resolve tickets within SLA standards (see Section J) via Service Now (Fuji user interface) through the OS/OCIO IT Service Desk.
- Maintain current, detailed HCHB network infrastructure diagrams and drawings.
- Establish maintenance agreements with the equipment manufacturer(s) for the backbone equipment that will allow advance replacements (expedited delivery of emergency replacements) for failed units/modules. These maintenance agreements shall cover Internetworking Operating System upgrades to ensure bug fixes and software releases are provided. The Government will procure CISCO smartnet through a separate contract vehicle. All other maintenance agreements will be reimbursable under the ODC CLIN.
- Provide customer service that can be monitored by relevant metrics to include, but not limited to reports on timeliness of response to service requests, effectiveness of communications, compliance with formal service desk ticket processing procedures, and the results of customer surveys.
- The Contractor shall also support moves, adds and changes for analog, IITSDN, T1, T3, special circuits, ATM from the local carrier for faxes, modems, elevator, and STE. Maintenance of HCHBNet wiring inside HCHB is also the Contractor's responsibility. If there is a failure of dial-tone from the local carrier, the NOC Contractor will coordinate with the Government prior to any maintenance. The NOC Contractor may also, with coordination with the Government, request a new line, new number or other service from the local carrier performed via an online portal. However, the analog phone service contract is between the Government and the local carrier, not with the NOC Contractor.
- Safeguard Government-provided property, including keys, sensitive data, personal computers, miscellaneous office equipment and furniture, and office/storage space, etc. Secure space for storage will be provided.
- Perform remedial maintenance after hours, during periods when it does not disrupt or impede the DOC customers.

SECTION C – DESCRIPTION/SPECIFICATIONS/STATEMENT OF WORK

- Provide administrative, analytical and implementation support to DOC customers for services offered under the WITS 2003, Networx and the GSA follow-on contract to WITS3 and Networx task orders. Provide consulting support to assist with the technical aspects of the disconnection and transition from WITS 2003 and Networx to the GSA follow-on contracts.
- Perform preventative network maintenance and upgrades on network hardware and tools to ensure that network is operating at optimal performance.
- Implement security patches and bug fixes to mitigate security vulnerabilities and known defects in accordance with best practices and to be in compliance with DOC security policies (see Section J).
- Provide artifacts to support Accreditation and Authorization activities.
- Review network aspects of building renovation design. Review GSA construction concepts, designs and other material and drawings as they relate to network and telecommunication renovation activities. Provide comments and recommendations with respect to network aspects of building renovation, i.e., cable plant, network servers, internetwork operating system, other network subsystems, racks, cable paths, power, cooling, monitoring, and security.
- Develop weekly activities reports and other reports in accordance with the task order deliverables requirement

SUBTASK 4.3.1: DATA CENTER SUPPORT

- Monitor all software and hardware products and ensure compliance to Data Center standards and best practices.
- Coordinate with IT Manager and other business units to develop strategies to ensure achievement of data center capacity.
- Analyze and determine appropriate layout of all equipment in data center for adequate power and cooling requirements.
- Monitor all data center activities such as new equipment installation or removal or disposal of existing equipment.
- Document all power and space schematics and ensure accuracy in same.
- Perform installation and ensure effective layout of all tools (Section J) in accordance to industrial standards and best practices.
- Monitor all data center assets for tracking and audit purposes.
- Coordinate with vendors and organization IT staff to ensure effective completion of all installation hardware.
- Perform capacity planning and power and cooling audits to ensure adequate power and cooling are supplied to service equipment.
- Maintain access control log to the data center and ensure appropriate filling of all columns in Sign-in sheet. Maintain Sign-in sheets for audit purposes.
- Monitor all issues and escalate issue as appropriate to specific IT organizations for prompt resolution.
- Ensure compliance with data center best practices and standards to ensure life safety is adequately provided and adhered to in the data center.

SECTION C – DESCRIPTION/SPECIFICATIONS/STATEMENT OF WORK

- Maintain standards of service levels at all times, ensure response with timeframe and manage all available services.
- Document Standard Operating Procedures and policies and best practices relating to data center operations.
- Attend HCHB Change Control Board meetings.
- Keep data center clean at all time and ensure compliance with appropriate use of data center.

SUBTASK 4.3.2: VOIP PHONES SUPPORT

- Operate and maintain existing Voice over Internet Protocol (VoIP) Phone System and its hardware and tools.
- Provide Moves, Adds and Changes (MAC) support on the Cisco and Unity Voicemail product for over 4,000 network and phone support users in HCHB. Ensure that phones are configured, registered to the phone management system and assigned to the right individuals. As appropriate, troubleshoot and resolve problems relating to the phones or phone management system.
- Document network characteristics for baseline and stability metrics and escalate troubles/problems to the NOC engineers.
- Coordinate moves with the building management staff as well as coordinate the activities of the NOC staff.
- Coordinate with the Local Exchange Carrier, Cisco, and other vendors.
- Serve as telecommunication tier 1 support for the customer on all telecom system performance (voicemail, fax line dial tone problem, Cisco IP phone device problem, Call accounting reporting).
- Troubleshoot technical problems with customer's phone device, voicemail and fax machine lines within HCHB.
- Interface and submit requests to Verizon WITS in reference to analog lines or trouble shooting DID line problems
- Update the CDR Infortel call accounting system and inventory of the active DID's or deactivated lines
- Provide and instruct users on the functionality of the Cisco IP phone product features, as well as with the Unity Voicemail product
- Ensure customer requests are routed to the proper NOC or IT group for resolution
- The VoIP technician will document all procedures, troubleshooting steps and SOW's related to this position. The VoIP technician will also update and verify existing support documentation and will work with the NOC team and ITCSC management.
- Input user information from Cisco Call Manager in order to reflect accurate reports for the line count report that is submitted annually for budgetary and charge back to customers.
- Semiannually review the Cisco Call Manager to ensure that the manager IDs are up to date to reflect office names.

SECTION C – DESCRIPTION/SPECIFICATIONS/STATEMENT OF WORK

C.4.4 TASK 4 – SECURITY OPERATIONS SUPPORT

- Actively monitor the HCHB network infrastructure and network audit logs for potential breaches in security and implement appropriate remediation. Remediate security problems identified by the Security Operations Center (SOC) or another responsible source.
- Provide real time monitoring and situational awareness of security events and first tier incident response and escalation to the DOC Enterprise Security Operations Center (ESOC) per DOC incident response policy and procedures.
- At least one member of the team shall be cleared at the Top Secret level to provide support to the DOC ESOC in response to classified security incidents detected via the Einstein Intrusion Prevention Security Services (IPSS).
- Maintain and enhance existing DLP capability and services to support active blocking of Personally Identifiable Information and any other information identified in DOC policies for the HCHB campus infrastructure and supported components and develop dashboard reporting elements for Senior and executive management;
- Manage and maintain security endpoint management solution for the Office of the Secretary and supported operating units.
- Conduct regular vulnerability scanning, reporting and assessment of OCIO supported systems.
- In coordination with the GTR and Managed Trusted Internet Protocol Services (MTIPS), review and manage security policies enforced at the MTIPS inspection Level for HCHB.
- Perform annual review and updates of policies for security tools on HCHBNet
- Note: On average, 25-30 scans are run a month

SUBTASK 4.4.1: NETWORK AND SECURITY ENHANCEMENTS

- Configure new network and security hardware and software to maximize the performance of the HCHB network infrastructure. No contractor furnished equipment is requested, equipment will be government owned/contractor operated. Develop Implementation/Upgrade Plan to include project schedule. Document new installations with screenshots to capture specific configuration and settings.
- Stay abreast of technology and recommend technology refreshment and/or new technology, including IT security awareness.
- Provide NOC on-site Continuity of Operations (COOP) support for relocated Office of the Secretary (OSEC) personnel at designated COOP locations. Note: the NOC does not provide a true COOP site; Operating Units and staff offices provide their own COOP plans and facilities. This is only relevant in a real world COOP event. NOC staff is not required to support annual COOP exercises.
- Provide Homeland Security Presidential Directive-12 (HSPD-12) implementation support. Make firewall rule and network changes so that Personal Identify Verification (PIV) cards can be used to authenticate users to the HCHB network infrastructure. The objective is to authenticate users to the Active Directory domain using PIV cards. The NOC Contractor shall only be responsible for the network tie-in and not the actual HSPD-12 or PIV cards implementation.

SECTION C – DESCRIPTION/SPECIFICATIONS/STATEMENT OF WORK

- Maintain and operate a Dual Stack IPv4 and IPv6 environment. Complete migration of HCHBNet to IPV6 from IPV4. This includes planning, testing and implementing IPV6 to the HCHB network infrastructure. The Contractor shall implement all routing and firewall rules to support IPV6.
- Maintain and operate Passive Optical Network (PON) that will be deployed as the HCHB building is being renovated. Anticipated PON deployment will be in the Renovation Phase 4 project scheduled to be operational sometime in March/April of 2018.
- Upgrade, replace and enhance existing HCHB-wide network infrastructure security equipment including the Intrusion Detection and Prevention Systems as part of Security Operations which will be provided as government furnished equipment.

SUBTASK 4.4.2: TESTING

- Provide routine maintenance, failover testing, and adjust or correct the HCHB network infrastructure outside normal working hours (after 9:00 p.m. during the week or on weekends as outlined in the Change Management Policy and Procedures and Standard Operating Procedures).
- Conduct complete testing of network software and hardware in the DOC lab and provide documented results to the Change Control Board for approval prior to implementing any change to the HCHBNet production environment.
- Test the Emergency Broadcast System (EBS) once each weekend, as a minimum, for technical correctness; and during core business hours once monthly, as a minimum, for functional correctness.
- Test the Public Address System after hours at least monthly to ensure technical correctness. The Contractor shall provide any required maintenance after regular business hours.

SUBTASK 4.4.3: PROCESS AND REPORTING

- Provide reports to the GTR and OCIO management that include:
 - Weekly, monthly, quarterly statistical reports that address the network performance goals and objectives in the SLAs (see Section J). All network support activities (e.g., trouble calls, service requests, special projects, scheduled maintenance, etc.), as well as reports concerning infrastructure system health, executive summary reports requested by the Government Task Manager and utilizing ServiceNow database and other sources; and,
 - Weekly, monthly, quarterly statistical data that address the HCHB network, VoIP and Emergency Broadcast system performance goals and objectives in the SLAs. The data shall include bandwidth utilization data, any service outages, historical service desk data (types of services provided, to whom, response times, Quality of service for the network/voice operations, PRI utilization, Security Audit Reports, etc.) and management reports.

SECTION C – DESCRIPTION/SPECIFICATIONS/STATEMENT OF WORK

- Develop, maintain and enforce Standard Operating Procedures (SOPs) for the NOC and SOC services rendered. Update the SOPs with the changes as appropriate. Comply with current and new SOPs.
- Conduct management briefings once a week.
- Maintain baseline of network utilization and performance metrics to include applications and traffic patterns.
- Continuously review the NOC and SOC operations and devise/report on ways to improve delivery of services and customer satisfaction.
- Provide monthly reports on Operating Units' telephone lines count.
- Provide quarterly HCHBNet node count reports.
- Comply with DOC Change Management Policy and Procedures and IT Security Policy (see Section J) provided in separate attachments.
- Maintain and update all NOC and SOC equipment inventory semiannually. All reporting is performed through GFE equipment. Follow SOPs for handling of equipment and inform DOC customer of equipment relocation/decommission. Assist OS property custodian with tracking of equipment per the DOC Property Inventory Audit.
- Maintain annual asbestos training for NOC Cable Infrastructure 5. Training will be provided by building management.
- Provide support and data on network and security configurations to the IT Security officer to remain in compliance with FISMA requirements with artifacts. This includes annual security Assessment and Authorization (A&A) activities and quarterly FISMA reports to the Office of Management and Budget (OMB).
- Maintain security patches on all NOC and SOC systems in accordance with DOC Security Policy (CITR-016 and CITR-017) (Section J).

C.4.5 TASK 5 – SYSTEMS ADMINISTRATION SUPPORT

C.4.5.1 SUBTASK 1 - TIER 3 SYSTEMS ADMINISTRATION SUPPORT

- Operate and manage the hardware, software and tools that support the Windows Active Directory environment.
- Deploy, manage and maintain Windows servers.
- Manage and maintain GPOs, Active Directory, DNS, File/Print server.
- Participates in technical research and development to enable continuing innovation within the infrastructure.
- Ensures system hardware, operating systems, software systems, and related procedures adhere to DOC standards.
- Install new/rebuild existing servers and configure hardware, peripherals, services, settings, directories, storage, etc. in accordance with standards and projects/operational requirements. All equipment is GFE.
- Develop and maintain installation and configuration procedures.
- Contribute to and maintain system standards.

SECTION C – DESCRIPTION/SPECIFICATIONS/STATEMENT OF WORK

- Research and recommend innovative, and where possible automated approaches for system administration tasks. Identify approaches that leverage resources and provide economies of scale.
- Perform daily system monitoring, verifying the integrity and availability of hardware, server resources, systems and key processes, reviewing system and application logs, and verifying completion of scheduled jobs such as backups.
- Perform regular security monitoring of systems to identify any possible intrusions.
- Provide Tier III support. Investigate and troubleshoot issues.
- Document SOPs on supporting the Active Directory environment.\
- Apply OS patches and upgrades to administrative tools and system in accordance to CINTR-016 or DOC and/or federally mandated requirements to address high to critical level vulnerabilities. BigFix and LanDesk are the current patching platforms. Maintain operational and configuration procedures.
- Perform periodic performance reporting to support capacity planning.
- Perform ongoing performance tuning, hardware upgrades, and resource optimization.
- Provide architecture and engineering support for customer applications, system interoperability and security.
- Provide support for DOC Office of Security (OSY) managed systems, including user access and backup considerations. Provide support to install, configure, upgrade, monitor, optimize and maintain application databases and regular patches.

SUBTASK 4.5.2: TIER 2 SYSTEMS ADMINISTRATION SUPPORT

- Provide support for account creation and deletion for approximate base of 1500 full service desk support users; average yearly creations: 632, deletions: 487 and modifications: 255.
- Analyze applications and network systems to plan, design, evaluate, and select operating systems and Desktop compatible components/peripherals. Responsible for assisting the Senior LAN Administrators with capacity planning, configuration assessment of workstations, laptops, mobile computing, NAS/SAN storage and other communications and peripheral devices.
- Provide support for new technologies to ensure interoperability with the LAN.
- Provide weekly statistics to upper management
- Develop and implement Standard Operating Procedures (SOPs) for the New Technologies.
- Establish secure computing environment by designing system configuration; directing system installation; defining, documenting, and enforcing system standards as they relate to the customer's desktop and mobile computing environment. This includes conducting site surveys, project meetings, installation and post-installation issues.
- Provide support of LAN equipment during outages, maintenance windows and equipment relocation. This task is usually performed after hours.

SECTION C – DESCRIPTION/SPECIFICATIONS/STATEMENT OF WORK

- Maximize effectiveness of the LAN environment by monitoring performance; troubleshooting operational problems and outages; scheduling upgrades; and developing processes on optimization.
- Provide support and account set up for the VPN access through the RSA system.
- Perform daily backup operations, ensuring all required file systems and system data are successfully backed up to the appropriate media, recovery tapes or disks are created, and media is recycled and sent offsite as necessary.
- Maintain and upgrade software elements, including the operating system
- Troubleshoot software and hardware issues
- Troubleshoot configuration problems
- Assist with maintenance of proper version of the installed software elements, including bug fixes and security
- Assist with data-spill cleanup, sanitization, and computer malware eradication in accordance with DOC and local policies and procedures with direction from DOC and security team
- Ensure that DOC is aware in writing of improperly performing equipment and assist on replacement/repair of such equipment
- Update and maintain desktop/laptop images on a regular basis or when new applications are added to the environment.

4.6 TASK 6 – IT SERVICE DESK SUPPORT

The contractor shall provide the expertise, technical knowledge, staff support and other related resources necessary to:

- Provide a Single Point of Contact (SPOC) for initial reporting of incidents
- Provide configuration, maintenance, and support for the existing ServiceNow (SNOW) Incident Management System (IMS) that integrates with existing DOC systems (such as LANdesk and BigFix) for incidents, requests and asset management. SNOW must be automated and aligned with Information Technology Infrastructure Library (ITIL) v3 standards. ServiceNow is government owned and contractor operated.
- Support for SNOW shall include the following nine modules:
 - Incident Management
 - Problem Management
 - Change Management
 - Knowledge Management
 - Release Management
 - Service Catalog
 - Configuration Management Database
 - Asset Management
 - Project Portfolio Management
- Process incidents/problems per defined SLAs
- Establish and maintain a Tier 0 self-service capability
- Provide Tier 1 on-site incident management support

SECTION C – DESCRIPTION/SPECIFICATIONS/STATEMENT OF WORK

- Provide Tier 2 on-site support for escalated tickets
- Provide management support to Tier 0, 1, and 2 operations
- Provide transition support and ensure continuity of operations
- Provide additional services, to include the following:
 - Surge projects and technology enhancements
 - Hardware and software purchases refresh activities
 - Travel to remote sites
 - Training support for ServiceNow feature enhancements which may include online or instructor-led sessions.
 - Extended hours of operation to support surge projects
 - Additional SLAs
 - Comprehensive application support
- Note: Annual total for first call resolution was 5,367 from a total of 25,819 calls for FY16.
- Note: No customer satisfaction rates have been measured to date
- Note: Mean time to respond and mean time to resolve metric for the past year are not available.

Tier 0, Tier 1, and Tier 2 activities are defined with the following tasks:

TIER	TASKS
Tier 0	<ul style="list-style-type: none">• Develop documentation, establish a self-service portal and associated knowledge base, and maintain updated information for users to obtain self-service such as FAQs and web-based entry of service requests• Current self-service and knowledge base is minimal and out dated. Expectation is contractor will expand both features and keep them current.• Tier 0 self-service capability exists but is not utilized and kept current.• Password reset may also be included in the self-service system
Tier 1 (on-site)	<ul style="list-style-type: none">• Serve as first point of contact for users• Log user calls, manage incoming service requests and incidents, create, update, and monitor all tickets• Track tickets until closure and update customer• Resolve all service requests that do not require escalation to higher tiers of service• Provide basic incident evaluation, fault isolation, analysis, and troubleshooting, resolving all incidents that do not require escalation to higher tiers of service• Use remote diagnosis and tools if applicable to resolve incidents• Escalate incidents to the appropriate tier based on SLA guidelines and dispatch on-site support as required
Tier 2 (on-site)	<ul style="list-style-type: none">• Resolve service requests that required escalation to Tier 2• Provide specialized/administrative on-site support: incident analysis, fault isolation, troubleshooting, and remedial/restoration actions after escalation to resolve ticket

	<ul style="list-style-type: none"> • Assist user with hardware incidents • Set up user accounts and workstations, provide scanning and virus remediation, manage loaner pool by configuration devices • Update tickets for all activities performed • Analyze trends and provide weekly management and user reports • Coordinate with external contractors for assets under warranty • Escalate incidents to the appropriate tier based on SLA guidelines • Image, test and deploy standard configurations for desktops and laptops. • Provide 24/7/365 support to DOC Secretary and staff.
--	---

SUBTASK 4.6.1: TECHNICAL MANAGEMENT SUPPORT

- Provide oversight of the IT Service Desk operations by ensuring adequate resources are assigned to resolve problems and issues in accordance with established SLAs.
- Provide weekly and monthly activities report to OCIO Task Manager.
- Provide pending tickets status.
- Interface regularly with other IT groups for situational awareness with upcoming projects and planned system maintenance.
- Attend meeting with OCIO Task Manager and management when requested.

SUBTASK 4.6.2: TIER 2 SUPPORT

- Conduct desk side visit with customers to resolve issues that cannot be addressed remotely.
- Repair and replace desktop/laptop hardware and parts where applicable.
- Install image, download drivers and application latest version and patches on desktops/laptops.
- Troubleshoot and resolve Windows Office applications.
- Perform regular file archival and purge as necessary.
- Create, change, and delete user accounts per request.
- Perform hardware maintenance on equipment that is maintained in-house
- Configure, install, and troubleshoot DOC-approved laptops, desktops, phones, tablets, network-connected multi-function devices, and other office IT equipment
- Configure, install, and troubleshoot DOC-approved software elements including the operating system (OS)
- Escalate hardware repair/replacement issues to DOC-contracted hardware vendors
- Ensure all portable IT equipment is current and ready for immediate deployment at all times
- Track status and whereabouts of all checked-out equipment and ensure checked-out equipment is returned on time. Loaner equipment should be secured and locked when not in use
- Support international travel program (includes device scanning, laptop wiping, and issuing of devices).
- Provide 24/7/365 support to DOC Secretary and staff.

SECTION C – DESCRIPTION/SPECIFICATIONS/STATEMENT OF WORK

SUBTASK 4.6.3: TIER 1 SUPPORT

The Contractor shall provide impact and priority-based incident categorization in order to track progress of all incidents and restore degraded or disrupted services as quickly as possible.

Contractor shall:

- Conduct initial triage and assign and escalate to other IT support organizations as appropriate.
- Provide a ITSD support structure that allows for escalation of incidents based on expertise required for resolution and urgency
- Answer customer telephone calls and emails to the ITSD in accordance with the applicable SLAs during normal working hours (NWH).
- Monitor all channels of incoming requests (emails, voicemails, submissions through the self-service portal)
- Log incidents and service requests into the IMS. Ensure that all incidents are promptly and accurately documented in IMS so that up-to-date information is available at all times. Track incidents from first report to remediation and closure.
- Perform initial diagnosis and analysis of Incidents and provide immediate resolution and recovery whenever possible. Use remote control tools to assist and resolve customer incidents as initial resolution, providing warm handoff escalation of Incidents that cannot be immediately resolved
- Escalate tickets as required
- Communicate system outages in accordance with established SOPs to appropriate DOC points of contacts and Users using DOC-provided tools and communication methods and continue ongoing communications until the Incident has been resolved and all services have been restored
- Follow-up on resolved Incidents to check quality, get customer concurrence of Incident closure, and to report customer satisfaction
- Work with Operational and other teams to ensure final summary, review, analysis, resolution, and lessons learned are documented in Incident Reports for all major Incidents and unplanned service outages, and submitted in writing to DOC management
- Establish and maintain and update information in the Known Error Database using existing material for reference; document workarounds and generate known error sub-processes to facilitate quicker diagnosis and resolution for future Incidents
- Proactively monitor Automatic Call Distribution (ACD) calls, Incidents and Service Request work flows, processes and queues to immediately identify and address performance issues that will impact the delivery of services to users
- Ensure non-IT requests are properly routed to appropriate support organizations.
- Provide live telephone coverage during NWH of service via a Contractor-owned call distribution system. All equipment will be GFE.
- Answer calls in the order they are received in accordance with applicable SLAs (see attached).
- Conduct triage support in accordance with Industry best practices.

SECTION C – DESCRIPTION/SPECIFICATIONS/STATEMENT OF WORK

- Continuously monitor the ITSD email queue for new requests or establish process/system to automatically route new requests to the ticketing system
- Create tickets in a manner that meets and/or exceeds applicable SLA
- Verify information with the end user, as required
- Provide user with a ticket number and record in ticket system
- Address any after-hours requests the next business day when NWH resume
- Update tickets in a manner that meets and/or exceeds applicable SLA
- Monitor critical events that come to the ITSD via any means, such as the network monitoring systems, phone call, e-mail, etc. These events could be associated with issues such as data spills or loss of data, customer unsatisfactory responses, and others determined to require immediate assistance and potential intervention.
- Make critical events available to all ITSD agents for real-time reference
- Create tickets and manage resolution process in a manner that meets and/or exceeds applicable SLA
- Update tickets by adding work log information as required by the applicable SLAs
- Monitor status of all open tickets and escalate as required
- Coordinate resolution with other internal and external teams, as appropriate
- Check the assigned tickets queue on regular basis throughout the NWH
- Provide advice and guidance to the Users regarding restoration of interrupted service
- Verify ticket resolution with the User
- Provide advice and guidance to Users regarding restoration of interrupted service.
- Require that no ticket be closed without concurrence from the User that the issue represented by the ticket has, in fact, been fully resolved and that the service has been restored. When an issue is resolved, the Contractor shall change status of the ticket to “Resolved”.
- Make no more than three (3) attempts within a six-day period to contact the User to secure an agreement to close the ticket.
- Assume all responsibility for resolving Incidents in a manner that meets or exceeds the applicable SLAs. It is the responsibility of the Contractor to escalate and/or seek assistance from DOC if other support teams are not being responsive to requests for assistance. The Contractor shall maintain status of all open tickets in a manner that meets the SLAs.
- Continuously review Incident data as well as other sources of information to identify trends that may lead to discovery of a common cause of incoming Incidents. When such a cause is determined, the Contractor shall create a Problem ticket and link all related Incident tickets to it. Upon resolution of the Problem ticket, the Contractor shall update all related Incident tickets.
- Log and track requests for IT components and services, and deliver approved IT components
- Log Service Requests into the IMS. Ensure that all Service Requests are promptly and accurately documented so that up-to-date information is available at all times
- Follow-up on completed requests to check quality, get customer concurrence of request closure, and to report customer satisfaction

SECTION C – DESCRIPTION/SPECIFICATIONS/STATEMENT OF WORK

- Establish (or update existing ones) and maintain an equipment checkout system for short-term assignments of laptops and other portable IT equipment
- Monitor processes that coordinate delivery of IT assets directly to customers and office equipment custodians. Ensure User in/out processing is factored into the process.
- Serve as the ticket “owner” of the resolution process from the initial contact with the Users to resolution of the Incident, Problem and Service Requests. The ITSD Contractor shall assume responsibility for Incident, Problem and Service Request resolution regardless of the party actually performing the work, i.e., if the work is performed by an organization external to the ITSD, the ITSD is still responsible to track the resolution and escalations, as required by the SLAs.
- Notify Users about planned maintenance windows and outages via user Broadcast emails. The Contractor shall make use of the ACD/Interactive Voice Response (IVR) system to notify Users about unscheduled service interruptions as soon as possible after the unscheduled service interruption is confirmed.

SUBTASK 4.6.4: TIER 0

- The Contractor shall establish and maintain a Tier 0 self-service capability for DOC users. This capability should include a knowledge base for user inquiries and help concerning commonly asked or requested services to be available on a self-service portal.
- DOC expects that a significant portion of today’s typical Tier 1 tickets can be diverted to Tier 0.
- The Contractor shall utilize existing materials as well as develop new documentation to use on the portal. Information shall be updated for users to obtain self-service such as FAQs and web-based entry of requests. Some documentation and FAQs may be posted on the DOC external website to assist users who are unable to log in to the system.
- The Tier 0 system may include a capability for password resets. Applications supported by the password reset system will be determined during the transition period.

C.4.7 TASK 7 – SERVER VIRTUALIZATION SUPPORT

- Operate and manage the hardware, software and tools (see Section J) that service the Server Virtualization environment.
- Operate and manage the SAN and Backup solution servicing the Server Virtualization environment.
- Build, configure and manage virtual machines.
- Configure and test all Windows server configurations in accordance with the appropriate NIST Security Configuration Checklist.
- Develop, implement, maintain and update Standard Operating Procedures (SOPs) for the Server Virtualization and its critical components.
- Provide node management, maintenance, and troubleshooting efforts for projects critical to the business.
- Provide technical leadership and mentoring to the virtualization team.
- Perform the operations daily health check to ensure that the network storage is operational.

SECTION C – DESCRIPTION/SPECIFICATIONS/STATEMENT OF WORK

- Provide Tier3 support in troubleshooting of the storage & virtualization network related issues and problems.
- Lead and coordinate troubleshooting.
- Resolve and close tickets in accordance with government/ customers SLAs.
- Ensure that the storage and its components are patched with the latest software version, security updates, and hotfixes.
- Conduct research on best practices to improve performance and enable storage/ virtualization environment stability and availability.
- Cross-train and mentor other engineers to improve coverage and team performance.
- Provide On-call rotation duty.
- Conduct after hours maintenance and troubleshooting as required.

C.4.8 TASK 8 – HSPD-12 PERSONAL IDENTIFICATION VERIFICATION SUPPORT

- Provide daily administration and operations support for windows authentication to approximately 1500 users using HSPD-12 Personal Identity Verification (PIV) cards.
- Provide compliance reports (bi-weekly) for PIV authentication enforcement.
- Utilize the Government provided Quest Migration Manager tools to perform all aspects of the Active Directory testing, implementation, recovery and account verification and integrity.
- Perform work on all phases of data security, quality control, data recovery and backup during the migration process.
- Configure and test all Windows server configurations in accordance with the appropriate NIST Security Configuration Checklist.
- Test, troubleshoot and resolve issues relating to PIV authentication.
- Provide enhancement support to integrate two-factor authentication for applications using PIV cards.

C.4.9 TASK 9 – BUILDING RENOVATION SUPPORT (OPTIONAL)

- Provide HCHB network and telecommunications implementation to support Building Renovation project. DOC's renovation will affect every space within the HCHB. Construction will take place throughout the Period of Performance of this Task Order. Throughout the life of the HCHB renovation project, the Contractor shall fulfill renovation network and telecommunication requirements.

The Building Renovation schedule is provided below:

Phase 1	<i>January 2008 – November 2009</i>	Replace air conditioning system cooling towers. Build the swing space to house staff while future phases of the building renovation are in progress.
Phase 2	<i>July 2009 – July 2012</i>	Interior and exterior renovations will encompass Corridor 1 along Constitution Avenue. This includes new mechanical, electrical, and plumbing systems, and architectural finishes (e.g., casework, molding, paneling). Phase 2 work also includes facade restoration and site utilities replacement around the entire

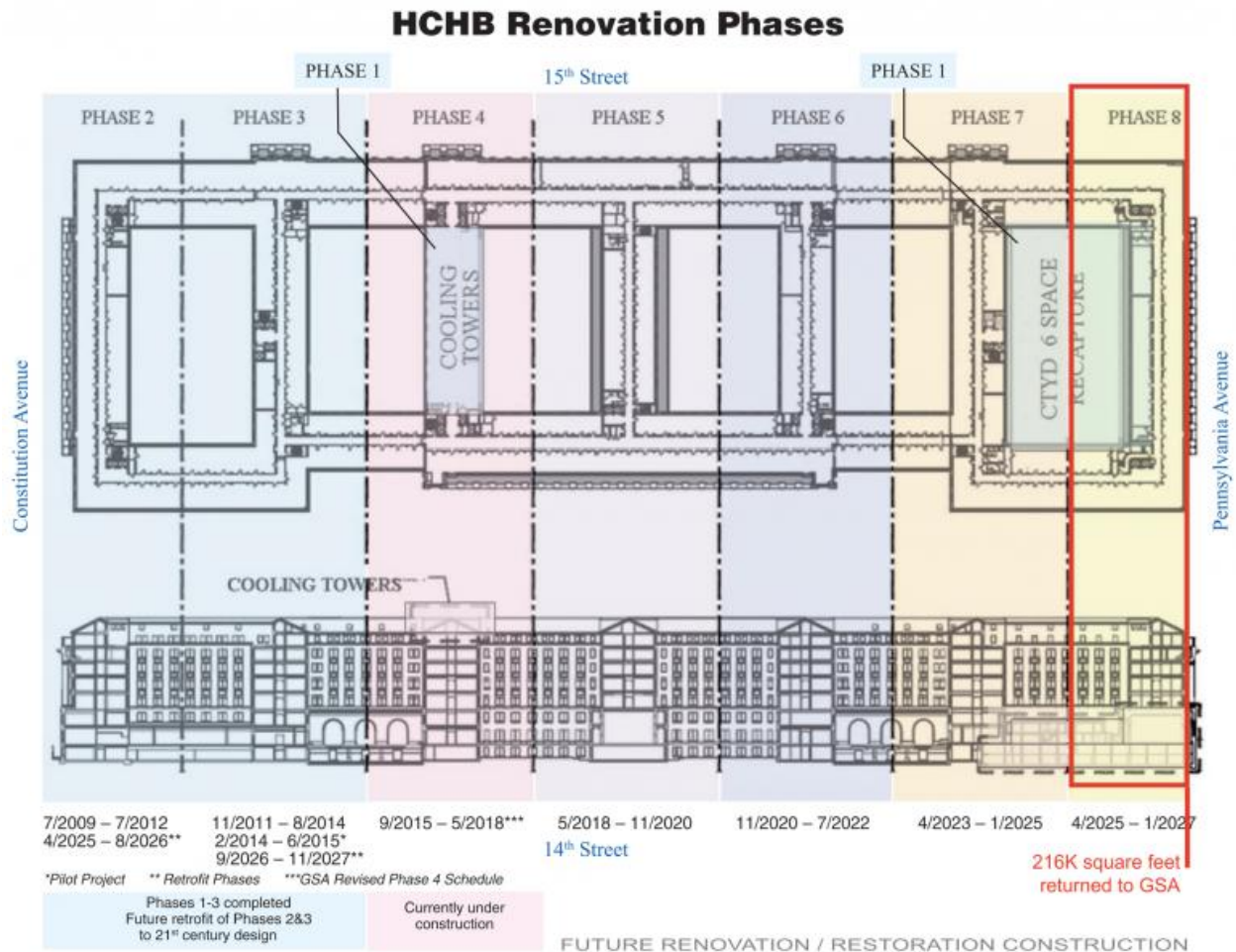
		building, and developing a staging area for construction materials. Staff moves out of Swing Space and Corridor 2 areas on June 15, 2012; moves will be complete by July 2012.
Phase 3	<i>November 2011 – August 2014</i> <i>Pilot Project:</i> <i>February 2014 – July 2015</i>	Interior and exterior flat roof renovations will encompass Corridor 2 (second corridor north of Constitution Avenue). This includes new mechanical, electrical, and plumbing systems, and architectural finishes. The DOC Federal Credit Union relocated to an area off the Reagan Building tunnel.
Phase 4	<i>September 2015 – May 2018</i>	Interior and flat roof renovations will encompass Corridor 3. This includes new mechanical, electrical, and plumbing systems, and architectural finishes. The Fitness Center relocated to the basement level, Corridor 3.
Phase 5	<i>April 2018 – November 2020</i>	Interior and flat roof renovations will encompass Corridor 4. This includes new mechanical, electrical, and plumbing systems, and architectural finishes.
Phase 6	<i>November 2020 – July 2022</i>	Interior and flat roof renovations will encompass Corridor 5. This includes new mechanical, electrical, and plumbing systems, and architectural finishes. Paper Clips will be relocated to the basement level, Corridor 5. The Child Care Center will be relocated.
Phase 7	<i>April 2023 – January 2025</i>	Interior and flat roof renovations will encompass Corridor 6. This includes new mechanical, electrical, and plumbing systems, and architectural finishes.
Phase 8	<i>April 2025 – January 2027</i>	Interior and exterior renovations will encompass Corridor 7 are. This space will be returned to GSA.
Retrofit Phase 2	<i>April 2025 – August 2026</i>	Update previously renovated space to 21st Century Workplace design.
Retrofit Phase 3	<i>September 2026 – November 2027</i>	Update previously renovated space to 21st Century Workplace design.

- The Contractor shall remove, replace, upgrade, and/or install cable plant, racks, panels, and other infrastructure associated with building renovation. Provide all network moves, additions and changes for all employees remaining in the HCHB, to include continuous HCHB network, telephone, emergency broadcast and desktop services during the renovation project. This includes the network cable plant up to the point of cable termination but excludes desktop devices (computers, telephone handsets, printers and other peripherals are excluded). The contractor shall provide miscellaneous materials such as cables, connectors and patch panels to support the move, add and change. These materials will be reimbursed through the ODC CLIN.
- The Contractor shall cooperate with other Government and contractor organizations participating in the renovation project, and shall ensure that network support does not adversely impact the renovation schedule.
- The Contractor shall perform network move, add and changes for areas that have been renovated. These renovated areas are issued Work Authorization form CD410t that identifies the required system furniture and supporting network cables layout. Work that

SECTION C – DESCRIPTION/SPECIFICATIONS/STATEMENT OF WORK

exceeds the threshold (10 new cables run per request) will be supported via this task. Cables installation of less than 10 new cables fall within the NOC Operational and Maintenance Support under Task 3.

- Contractor shall provide support with the planning and execution required to successfully relocate network equipment to prevent damages to these devices. Contractor shall perform these tasks during approved maintenance window to ensure minimal disruption to NOC services.
- Contractors shall provide support with the planning and execution to successfully relocate networking equipment and services from A001 to the new NOC Secondary Core Room in the Phase 5 (Corridor 4) areas. Contractor shall establish network connectivity from the new NOC Secondary Core Room to existing Telecommunications closets.
- Conduct Quality Assurance for all fibers and copper cables installed in the renovated areas. The Contractor shall test and validate that the fibers and cables are properly implemented in accordance with standards and procedures and in compliance with other governing regulations and policies.
- Survey the areas to be renovated and if required, establish network connectivity for users impacted by the decommissioning of the telecommunication closets located in those areas.



C.4.10 TASK 10 - CLOUD MIGRATION SUPPORT (OPTIONAL)

The Contractor shall provide engineering and new technologies implementation. The Contractor shall provide hardware, software, and process innovations that depart from the existing technical architecture and so are within the scope of Task 10.

- Provide technical support for migration of DOC/OCIO applications, data, and other resources to the cloud. This includes research and development, design and migration support to ensure successful migration to the cloud.
- Develop an engineering and design plan to migrate the virtualized server environment to the cloud. Assist with the migration effort to minimize services disruption.
- Note: Excluded are the cloud platforms, which DOC/OCIO will procure from another source or which the Contractor will purchase under the ODC Ancillary Products/Service CLIN.
- Note: Innovation environments within vendor's labs is permitted if on the vendor's time, equipment and funded by the vendor.
- Note: Both on premise and public cloud solutions will be considered

SECTION C – DESCRIPTION/SPECIFICATIONS/STATEMENT OF WORK

C.4.11 TASK 11 – NEW TECHNICAL ARCHITECTURE AND TECHNOLOGIES IMPLEMENTATION (OPTIONAL)

The Contractor shall provide engineering and new technologies implementation. The Contractor shall provide hardware, software, and process innovations that depart from the existing technical architecture and so are within the scope of Task 11.

- Identify, analyze, develop, plan and propose for deployment new or emerging technical architectures that depart from the current DOC/OCIO technical architecture. Document this analysis and plans for DOC/OCIO management consideration.
- Implement new technical architecture consistent with DOC/OCIO guidance. Examples: central server to client server; centralized to distributed; proprietary to open systems; web enabling systems and applications; Windows to Linux; independent to consolidated networks; other topological changes.
- Develop an engineering and design plan to migrate from the existing Capital Expenditure (CAPEX) model to an Operating Expenditure (OPEX) model.
- Develop a plan to standup a redundant site to support HCHBNet services. Once the redundant site is operational, ongoing management and support of the redundant site will be part of Task 3.
- Implement new technologies/solution to comply with new Office of Management and Budget (OMB) mandates and other federally mandated requirements to address critical vulnerabilities. Gather requirements and provide technical support to ensure successful compliance with these new OMB mandates.
- Allow for future growth and implementation of new technology, as it becomes available, and recommend operational improvements and architectural changes.
- Refresh new desktops and laptops which are outside of the normal desktops/laptops replacement/refresh activities identified under Task 5: IT Service Desk Support. All equipment will be GFE.
- Note: Excluded are the cloud platforms, which DOC/OCIO will procure from another source or which the Contractor will purchase under the ODC Ancillary Products/Service CLIN.
- Note: Innovation environments within vendor's labs is permitted if on the vendor's time, equipment and funded by the vendor.

C.4.12 TASK 12 – AUDIO VISUAL AND VIDEO TELECONFERENCING (VTC) O & M SUPPORT

The contractor will provide support to ensure that the audio visual and video teleconferencing systems are operating at optimal level.

- Support daily VTC operational and maintenance activities to include conducting daily health check of VTC system and components. Respond to ticket assignments and provide resolution.

SECTION C – DESCRIPTION/SPECIFICATIONS/STATEMENT OF WORK

- Execute all aspects of videoconferencing including call setup, end user training, troubleshooting, and follow through on escalation of trouble incidents occurring during calls;
- Respond to client service desk calls for support, troubleshooting, or other requests covered under the client agreement;
- Perform VTC testing to include connectivity testing of local VTC units in the HCHB campus with remote VTC connections.
- Lead or assist in the support (hands-on if necessary) of special events, high profile senior executive meetings, town halls requiring videoconferencing as directed by the client;
- Provide technical consultation, support, and act as lead contact for all videoconferencing operations and maintenance;
- Solve all technical issues related to telepresence infrastructure and endpoints with minimal downtime;
- Setup WebEx sessions for remote users that are not able to participate in meetings via video conferencing
- Perform quarterly engineering analysis of requirements for videoconference support and provide recommendations of preferred solutions that optimize engineering, management, and cost parameters;
- Maintain usage statistics, issue and repair logs, or other collection/reporting systems;
- Create and modify user documentation and standard operation procedures. Review and update of the documentation shall be performed on an annual basis at minimum and with each major change to systems being managed.

C.4.13 TASK 13 - LIVE WEBCAST STREAMING SUPPORT (OPTIONAL)

- Provide Production Services to include:
 - Contractor must provide all personnel and equipment necessary to produce live webcasting events currently estimated at four events per year and have an understanding of audio/video formats and encoding processes. Production includes all meetings and preparations necessary to identify and set-up required resources (both government and contractor resources) prior to the event, support during event, recording and broadcast of event and wrap up, post-event.
 - Events must be 508 compliant and accessible
 - Inclusive in services is project management to oversee all pre-, event and post-event activities
 - Contractors must be capable of providing production services within the HCHB campus area only.
 - Contractors should be able to provide single- or multi-camera recording capability
- Provide Registration Services to include:

The webcast portal will allow the government to customize the registration fields beyond the basic requirements (first name, last name, organization, email address, business phone number).

 - Customized registration confirmation, event updates, event reminders and thank you emails will be offered through the contractor's webcasting portal. The government

SECTION C – DESCRIPTION/SPECIFICATIONS/STATEMENT OF WORK

- will have access to the webcasting portal or personnel to upload the preferred email communications. The government will provide details on timing of communications.
- Provide Broadcast Capability Services to include:
 - The contractor will provide a live webcasting portal website to support a maximum of up to 45,000 concurrent viewers. An estimated 4 events are to occur per year. The Contractor should have the live portal available at least 5 days before the event.
 - The webcasting portal will be made available via a personalized website link; will be offered in but not limited to Windows Media Player®, Adobe Flash® and RealPlayer® (or current popular media players); and will stream live from the Internet with no additional plug-ins.
 - The webcasted sessions shall support the minimum bit rate for delivery of quality sessions that can be viewed
 - The webcasting portal shall be viewable on a variety of desktop, laptop, smart phone and tablet devices and all popular browsers to include but not limited to (Internet Explorer, Chrome, Firefox, Safari, etc.)
 - The webcasting portal shall allow the presenter and/or government to upload presentations in Microsoft Office Suite of products to include but not limited to Microsoft PowerPoint, Word, Excel or PDF format
 - The webcasting portal will be customizable with government provided event branding and graphics, such as a web banner.
Furthermore, the contractor shall provide a webcasting portal URL for the government to include on DOC websites that will be active during the event and for the duration of the archive period.
 - The webcasting portal will offer the viewers the ability to live chat with other viewers. Viewers will be able to conduct private chats with other viewers or chat in a community setting within the presentation portal.
 - Contractors must provide optional moderated audience Q&A capabilities during and live polling events
- Provide Archiving/File Formats Services to include:
Post-event, contractor must provide archived versions of the event to the government in a format as required by the customer. Formats may include: DVD, Blue Ray, CD, USB or internet formats
 - Archived events on the webcasting portal and those delivered to the government must be transcribed so as to be 508-compliant. The following website provides information on Section 508 compliance: <http://www.howto.gov/web-content/accessibility/508-compliant-and-accessible-multimedia>.
- Provide Event Reporting Services to include:
The webcasting portal shall capture and provide the following reports:
 - Registration statistics;
 - Number of viewers for each presentation;
 - The length of time each viewer views each presentation;
 - Total number of unique registered viewers for the entire webcasting event per day;
 - Archived presentation viewer data.
- Security Requirements: The Hosting site shall be FIPS compliant and support security of email transmittal if email transmittal is required as part of the service.

SECTION C – DESCRIPTION/SPECIFICATIONS/STATEMENT OF WORK

C.4.14 COOPERATION (ALL TASKS)

The success of this Task Order is largely dependent on the willingness and ability of the Contractor to cooperate fully with other stakeholders. The Contractor shall cooperate fully with OCIO, other DOC staff and contractors, and with staff and contractors at other DOC Operating Units; share information; openly discuss issues and concerns; and work towards the common resolution of issues and problems and accomplishment of DOC missions. Network and telecommunications support includes support service integration (e.g., integration of all the support tasks in this task order).

The Contractor's staff shall be fully instilled with the skills to provide excellent customer service and a high degree of cooperation with the Government and other support contractors.

SECTION D – PACKAGING AND MARKING

D.1 PRESERVATION, PACKAGING AND MARKING

All deliverables submitted to the Government shall indicate the contract number, TO number, contractor's name, description of items contain therein and the consignee's name and address for which the information is being submitted. The contractor shall follow the marking requirements specified by the Government.

All reports and deliverables should be submitted electronically through GSA's electronic contract system (ITSS) at:

<https://portal.fas.gsa.gov/group/aasbs-portal/itss-home>

Identified below are the required electronic formats, whose versions must be compatible with the latest, commonly available version on the market.

- | | |
|----------------|----------------------|
| • Text | Microsoft Word |
| • Spreadsheets | Microsoft Excel |
| • Briefings | Microsoft PowerPoint |
| • Drawings | Microsoft Visio |
| • Schedules | Microsoft Project |
| • PDF | Adobe Acrobat Reader |

Copies of all deliverables shall also be delivered electronically to the DOC Government Technical Representative (GTR) in a Microsoft format. The GTR will be provided upon award.

SECTION E – INSPECTION AND ACCEPTANCE

E.1 PLACE OF INSPECTION AND ACCEPTANCE

Inspection and acceptance of all work performance, draft reports, and other deliverables under this TO shall be performed by the Government Technical Representative (GTR) and/or Contracting Officer Representative (COR).

E.2 SCOPE OF INSPECTION

All deliverables will be inspected for content, completeness, accuracy and conformance to this TO requirements by the Government Technical Representative and/or COR. Inspection may include validation of information or software through the use of automated tools, testing or inspections of the deliverables, as specified in the TO. The scope and nature of this inspection will be sufficiently comprehensive to ensure the completeness, quality and adequacy of all deliverables.

The Government requires a period not to exceed fifteen (15) work days after receipt of final deliverable items for inspection and acceptance or rejection.

E.3 BASIS OF ACCEPTANCE

The basis for acceptance shall be compliance with the requirements set forth in the Task Order, the contractor's proposal and other terms and conditions of the task order including the Government Quality Surveillance Plan (QASP) (see Section J). Deliverable items rejected shall be corrected in accordance with the applicable clauses.

Reports, documents and narrative type deliverables will be accepted when all discrepancies, errors or other deficiencies identified in writing by the Government have been corrected.

If the draft deliverable is adequate, the Government may accept the draft and provide comments for incorporation into the final version.

All of the Government's comments to deliverables must either be incorporated in the succeeding version of the deliverable or the contractor must demonstrate to the Government's satisfaction why such comments should not be incorporated.

If the Government finds that a draft or final deliverable contains spelling errors, grammatical errors, improper format, or otherwise does not conform to the requirements stated within this Task Order, the document may be immediately rejected without further review and returned to

SECTION E – INSPECTION AND ACCEPTANCE

the contractor for correction and resubmission. If the contractor requires additional Government guidance to produce an acceptable draft, the contractor shall arrange a meeting with the GSA COR.

E.4 DRAFT DELIVERABLES

The Government will provide written acceptance, comments, and/or change requests, if any, within 15 workdays from Government receipt of the draft deliverable. Upon receipt of the Government comments, the contractor shall have ten workdays to incorporate the Government's comments and/or change requests and to resubmit the deliverable in its final form.

E.5 WRITTEN ACCEPTANCE/REJECTION BY THE GOVERNMENT

The Government will provide written notification of acceptance or rejection of all final deliverables within 15 work days unless specified otherwise. All notifications of rejection will be accompanied with an explanation of the specific deficiencies causing the rejection.

E.6 NON-CONFORMING PRODUCTS OR SERVICES

Non-conforming products or services will be rejected. Deficiencies will be corrected, by the contractor, within 10 work days of the rejection notice. If the deficiencies cannot be corrected within ten (10) work days, the contractor will immediately notify the GSA COR of the reason for the delay and provide a proposed corrective action plan within 10 work days.

SECTION F – DELIVERABLES OR PERFORMANCE

F.1 TASK ORDER PERIOD OF PERFORMANCE

The period of performance for this TO is a seven (7) month base period with four (4) 1-year option periods. The period of performance during the base period for Task 6 IT Service Desk and Task 12 Audio Visual and VTC O&M Support will commence after task order award as follows:

Task 6 IT Service Desk	09/15/2017
Task 12 Audio Visual and VTC O&M Support	08/15/2017

The period of performance for the base period begins on date of award. The transition-in period of one month begins immediately upon task order start date. The transition-out period will begin two months prior to the end of the task order.

F.2 PLACE OF PERFORMANCE

The Government Site is the principal place of performance. The Work performed by the contractor under this TO shall be performed at the Department of Commerce, Office of the Chief Information Officer, 14th & Constitution Ave. NW, Washington DC 20230. Periodic visits may be needed to other DOC locations. All offices requiring visits will be located in the National Capital Region.

F.3 CORE HOURS OF OPERATION

The contractor is responsible for conducting business, between the hours specified below, Monday thru Friday except Federal holidays or when the government facility is closed due to local or national emergencies, administrative closings, or similar government directed facility closings. The contractor must at all times maintain an adequate workforce for the uninterrupted performance of all tasks defined within this TO when the Government facility is not closed for the above reasons. When hiring personnel, the contractor shall keep in mind that the stability and continuity of the workforce are essential. The contractor may be asked to be available for on-call emergencies.

The hours of operations are as followed:

TASK	DESCRIPTION	HOURS OF OPERATION
2	Program/Project Management	8AM - 5PM EST Monday - Friday except Government Holidays
3	Network Operations	7AM - 6PM EST Monday - Friday except Government Holidays
4	Security Operations	7AM - 6PM EST Monday - Friday except Government Holidays
5	Systems Administration	8AM - 5PM EST Monday - Friday except Government Holidays
6	IT Service Desk – Tier 1	6AM - 10PM EST Monday - Friday except Government Holidays
6	IT Service Desk – Tier 2	7:30AM - 6PM EST Monday - Friday except Government Holidays 24/7/365 support to DOC Secretary and staff

7	Server Virtualization	8AM - 5PM EST Monday - Friday except Government Holidays
8	PIV Support	8AM - 5PM EST Monday - Friday except Government Holidays

F.4 DELIVERABLES

The following schedule of milestones will be used by the COR to monitor timely progress under this TO. The contractor shall provide the following documentation in the milestone list and maintain version control throughout the life of the application, unless otherwise specified by the COR.

The following abbreviations are used in this schedule:

NLT – No Later Than

PS – Project Start

PMP – Project management Plan

QCP – Quality Control Plan

All references to Days: Government Workdays except as specifically noted.

Deliverables are due the next Government workday if the due date falls on a holiday or weekend. The Contractor, at the Governments discretion, may be required to provide the following deliverables (the due date for all deliverables shall be negotiated with government based on schedule and performance unless otherwise noted):

MILESTONE/DELIVERABLE	REFERENCE	PLANNED COMPLETION DATE
Project Start (PS)		
Transition In Plan – Draft	C.4.1.1	Due at Kickoff Meeting
Transition In Plan - Final	C.4.1.1	10 Days after receipt of Government Comments
Transition Out Plan Draft	C.4.1.2	NLT 90 days before Task Order expiration
Transition Out Plan - Final	C.4.1.2	10 Days after receipt of Government Comments
Kickoff Meeting	C.4.2.1	Within 5 days of award
Monthly Status Reports	C.4.2.2	Monthly, 10th calendar day of the next month
Weekly Technical Status Report	C.4.2.3	Weekly, Wednesday by 9:30 a.m.
Project Management Plan - Draft	C.4.2.4	NLT 20 days after kickoff meeting and then annually for updates
Project Management Plan - Final	C.4.2.4	10 days after receipt of Government Comments
Project Management Plan Updates	C.4.2.5	At least annually
QCP - Draft	C.4.2.6	NLT 20 days after kickoff

MILESTONE/DELIVERABLE	REFERENCE	PLANNED COMPLETION DATE
		meeting
QCP - Final	C.4.2.6	10 Days after receipt of Government Comments
QCP - Updates	C.4.2.6	At least annually
Network Hardware Installation Documentation	C.4.3	At the time of Installation
Network Maintenance Documentation	C.4.3	Prior to Network Maintenance Activity
Network Infrastructure Diagrams and AutoCad Drawings	C.4.3	NLT 10 days after changes are made
Network, VOIP, and EBS Performance Statistical Reports	C.4.3	Weekly, Monthly, Quarterly
Vulnerability scanning and reporting	C.4.4	Monthly
Work Breakdown Structure	C.4.10, C.4.11	NLT 10 days after need is identified
Network Engineering Studies, Design and Engineering Plan for Virtual Server Migration	C.4.10	NLT 20 days after optional CLIN is exercised
New Technical Architecture Documentation	C.4.11	NLT 10 days after emerging technology is identified
Provide archived versions of events and viewer data	C.4.13	NLT 10 days after event
Daily Health Check	C.4.3, C.4.4, C.4.5, C.4.6 C.4.7, C.4.8	Daily
Software and Hardware Test Result Documentation	All tasks	Prior to Implementing Any Change
System Performance and Utilization Reports	All Tasks	Weekly, Monthly, Quarterly
New Technology Recommendations	All Tasks	As New Technology Becomes Available
Standard Operating Procedure Updates	All Tasks	As appropriate as changes are made
Initial IT Security Orientation Training	H.9(f)	NLT 10 days after task order award
Provisions Acknowledgment	H.9(g)	NLT 10 days after task order award
System Certification Work Plan	H.9(1)	NLT 14 days after task order award
System Security Plan and Certification Documentation	H.9(2)	NLT 14 days after approval from Government

SECTION F – DELIVERABLES OR PERFORMANCE

F.5 PUBLIC-RELEASE OF CONTRACT DOCUMENTS REQUIREMENT

The contractor agrees to submit, within ten (10) workdays from the date of the CO's execution of the initial TO, or any modification to the TO (exclusive of Saturdays, Sundays, and Federal holidays), a portable document format (PDF) file of the fully executed document with all proposed necessary redactions, including redactions of any trade secrets or any commercial or financial information that it believes to be privileged or confidential business information, for the purpose of public disclosure at the sole discretion of GSA. The contractor agrees to provide a detailed written statement specifying the basis for each of its proposed redactions, including the applicable exemption under the Freedom of Information Act (FOIA), 5 U.S.C. § 552, and, in the case of FOIA Exemption 4, 5 U.S.C. § 552(b) (4), shall demonstrate why the information is considered to be a trade secret or commercial or financial information that is privileged or confidential. Information provided by the contractor in response to the TO requirement may itself be subject to disclosure under the FOIA. Submission of the proposed redactions constitutes concurrence of release under FOIA.

GSA will carefully consider the entire contractor's proposed redactions and associated grounds for nondisclosure prior to making a final determination as to what information in such executed documents may be properly withheld.

F.6 DELIVERABLE MEDIA

The following are the required electronic formats unless stated otherwise, whose versions must be compatible with the latest, commonly available version on the market.

a. Text	MS Word
b. Spreadsheets	MS Excel
c. Briefings	MS PowerPoint
d. Drawings	MS Visio
e. Schedules	MS Project

SECTION F – DELIVERABLES OR PERFORMANCE

F.7 PLACE(S) OF DELIVERY

Unclassified deliverables or correspondence shall be submitted electronically through ITSS at the following address:

<http://www.gsa.gov/portal/content/101033>

An electronic copy of all deliverables shall also be submitted to the Government's Technical Representative Point of Contact. The GTR will be provided at time of award.

F.8 NOTICE REGARDING LATE DELIVERY

The Contractor shall notify the GSA COR, as soon as it becomes apparent to the Contractor, that a scheduled delivery will be late. The Contractor shall include in the notification the rationale for late delivery, the expected date for the delivery and the project impact of the late delivery. The GSA COR will review the new schedule and provide guidance to the Contractor. Such notification in no way limits the Government's right to any and all rights and remedies up to and including termination.

SECTION G – CONTRACT ADMINISTRATION DATA

G.1 CONTRACTING OFFICER’S REPRESENTATIVE (COR)

The Contracting Officer will appoint a COR in writing through a COR Letter of Appointment that will be provided to the contractor upon award. The COR will receive, for the Government, all work called for by the TO and will represent the CO in the technical phases of the work. The COR will provide no supervisory or instructional assistance to contractor personnel.

The COR is not authorized to change any of the terms and conditions, scope, schedule, and price of the TO. Changes in the scope of work will be made only by the CO by properly executed modifications to the contract.

G.2 TASK ORDER CPARS

The TO performance will be evaluated and captured through the CPARS module (located at <https://www.cpars.gov/>). At a minimum, the TO performance will be evaluated by GSA upon contract completion at a minimum annually. Evaluations of contractor performance will be provided to the contractor as soon as practicable after completion of the evaluation. Contractors will be given a minimum of 30 days to submit comments, rebutting statements, or additional information. Copies of the evaluations, contractor responses, and review comments, if any, will be retained as part of the contract file, and may be used by Federal agencies to support future award decisions.

G.3 CONTRACT ADMINISTRATION

Contract Specialist:

Daniel Miller
GSA FAS AAS NCR, Region 11
301 7th Street, SW, Room 6109
Washington DC, DC 20407-0000
Telephone: (703)328-7948
Email: Daniel.R.Miller@gsa.gov

Contracting Officer:

Reva Hutchinson
GSA FAS AAS NCR, Region 11
301 7th Street, SW, Room 6109
Washington DC, DC 20407-0000
Telephone: (202)708-1253
Email: reva.hutchinson@gsa.gov

SECTION G – CONTRACT ADMINISTRATION DATA

Contracting Officer's Representative:

Julius Bradshaw
GSA FAS AAS NCR, Region 11
301 7th Street, SW, Room 6109
Washington DC, DC 20407-0000
Telephone: (202)708-5933
Email: julius.bradshaw@gsa.gov

Government Technical Representative (GTR)

TBD

G.4 INVOICE SUBMISSION

The contractor shall submit invoices electronically in the IT Solutions Shop (ITSS) at <https://portal.fas.gsa.gov>. The contractor shall certify with a signed and dated statement that the invoice is correct and proper for payment. In addition, the contractor shall provide invoice backup data in accordance with the contract type, including detail such as labor categories, rates, and quantities of labor hours per labor category.

G.5 INVOICE REQUIREMENTS

A proper invoice shall be submitted monthly and not later than 5 work days after acceptance by the Government of the product, service, and/or cost item. A separate invoice for each TO shall be submitted on official company letterhead with detailed costs for each of the following categories:

1. Total labor charges
2. Travel and per diem charges
3. Total other direct charges (ODC)
4. Total invoice amount
5. Prompt payment discount offered (if applicable)

For other direct costs such as equipment, travel, per diem, subcontractor labor, etc., invoices shall reflect the contractor's actual expense for the item, plus General and Administrative charges (G&A) These charges shall not exceed limits specified in the TO. No charges will be paid by the Government that are not specifically detailed in the individual TO and specifically approved in the underlying contract. Copies of contractor paid invoices, receipts, and travel vouchers completed in accordance with Federal Travel Regulations (FTR) shall be maintained by the contractor and made available to the Government upon request.

In addition to the above information, all invoices must include the following:

1. Task Order ID
2. Delivery Order Number
3. GSA ACT# for proper identification
4. Period of Performance (month services performed for work request task orders, month deliverable completed for fixed price task orders)

SECTION G – CONTRACT ADMINISTRATION DATA

5. Invoice Number
6. Client Name and address

Failure to include this information may result in the Contractor having to resubmit the invoice and delaying payment.

Invoices for final payment must be so identified and submitted when services have been completed and no further charges are to be incurred. These close-out invoices, or a written notification that final invoicing has been completed, must be submitted to GSA within 30 days of order completion. A copy of the written acceptance of completion must be attached to final invoices. If the Contractor requires an extension of the 30-day period, a request with supporting rationale must be received by GSA prior to the end of the 30-day period.

G.5.1 FIRM-FIXED PRICE (FFP) CLINs

The contractor may invoice as stated in Section B – Supplies or Services and Price/Costs for the FFP CLINs on a monthly basis. The invoice shall include the period of performance or deliverable/progress payment period covered by the invoice and the CLIN number and title. All costs shall be reported by CLIN element (as shown in Section B – Supplies or Services and Price/Costs) and shall be provided for the current invoice and in total from project inception to date. The contractor shall provide the invoice data in spreadsheet form with the following detailed information. The listing shall include separate columns and totals for the current invoice period and the project to date.

1. FFP (insert period of performance or deliverable/progress payment period – as stated in Section B – Supplies or Services and Price/Costs)
2. Cost incurred not billed

G.5.2 LABOR HOUR (LH) CLINs

The contractor may invoice monthly on the basis of cost incurred as stated in Section B – Supplies or Services and Price/Costs for the FFP CLINs on a monthly basis. All hours and costs shall be reported by CLIN element (as shown in Section B), by application, by contractor employee, and shall be provided for the current billing month and in total from project inception to date. The contractor shall provide the invoice data in spreadsheet form with the following detailed information. The listing shall include separate columns and totals for the current invoice period and the project to date.

1. Employee name (current and past employees)
2. Employee company labor category
3. Employee Alliant Small Business labor category
4. Monthly and total cumulative hours worked
5. Corresponding TO ceiling rate
6. Cost incurred not billed

All cost presentations provided by the contractor shall also include Overhead charges, and General and Administrative charges and shall also include the Overhead and General and Administrative rates being applied.

SECTION G – CONTRACT ADMINISTRATION DATA

G.5.3 ODCs

The contractor may invoice monthly on the basis of cost incurred for the ODC CLIN. The invoice shall include the period of performance covered by the invoice and the CLIN number and title. In addition, the contractor shall provide the following detailed information for each invoice submitted, as applicable. Spreadsheet submissions are required.

1. Tools and/or ODCs purchased.
2. Consent to Purchase number or identifier.
3. Date accepted by the Government.
4. Associated CLIN.
5. Project-to-date totals by CLIN.
6. Cost incurred not billed.
7. Remaining balance of the CLIN.

All cost presentations provided by the contractor shall also include Overhead Charges, General and Administrative Charges and Fee.

G.5.4 TRAVEL

Long distance travel is travel over 50 miles. Local travel will not be reimbursed. Contractor costs for travel will be reimbursed at the limits set in Federal Travel Regulation (FTR) (see FAR 31.205-46):

1. Joint Travel Regulation (JTR) – prescribed by the GSA, for travel in the contiguous U.S.

The contractor may invoice monthly on the basis of cost incurred for cost of travel. The invoice information shall identify all cumulative travel costs billed by CLIN. The current invoice period's travel details shall include separate columns and totals and include the following:

1. Travel authorization request number or identifier, approver name, and approval date.
2. Current invoice period.
3. Names of persons traveling.
4. Number of travel days.
5. Dates of travel.
6. Number of days per diem charged.
7. Per diem rate used.
8. Total per diem charged.
9. Transportation costs.
10. Total charges.
11. Explanation of variances exceeding 10% of the approved versus actual costs.
12. Indirect handling

All cost presentations provided by the contractor shall also include Overhead charges and General and Administrative charges.

SECTION H – SPECIAL CONTRACTS REQUIREMENTS

H.1 KEY PERSONNEL

The following are the minimum personnel who shall be designated as “Key.” The Government does not intend to dictate the composition of the ideal team to perform this contract. Therefore, the Government encourages and will evaluate additional Key Personnel as proposed by the offeror.

- Project Manager (PM)

The Government desires that Key Personnel be assigned for the duration of the contract.

H.1.1 PROJECT MANAGER

The Contractor shall identify a Project Manager (PM) to serve as the Government’s major point-of-contact and to provide overall leadership and guidance for all Contractor personnel assigned to the Task Order. The PM is ultimately responsible for the quality and efficiency of the Task Order to include both technical issues and business processes. The PM shall assign tasking to Contractor personnel, supervise on-going technical efforts, and manage overall Task Order performance.

This individual shall have the ultimate authority to commit the Contractor’s organization and make decisions for the Contractor’s organization in response to Government issues, concerns, or problems. This person shall be readily available to respond to Government questions, concerns, and comments, as well as be proactive in alerting the Government to potential contractual or programmatic issues.

It is required that the PM has the following qualifications:

1. Project Management Professional Certification (PMP) from PMI with a minimum of 8 years of experience
2. ITILv3, CCNA, CCNP or technical Certification
3. Demonstrated experience in the management, operations, maintenance and enhancement of information technology networks similar to HCHBnet in terms of hardware, software, topology and complexity.
4. Demonstrated experience managing network installation, upgrades or renovation projects; system security projects; and system engineering or enhancement projects.
5. Demonstrated experience managing system administration, security, operations, hardware and software acquisition and maintenance, and configuration management functions.

H.1.2 KEY PERSONNEL SUBSTITUTION

The contractor shall not replace any personnel designated as Key Personnel without the written concurrence of the CO. Prior to utilizing other than personnel specified in proposals in response to this TOR, the contractor shall notify the GSA CO and the GSA COR of the existing TO. This notification shall be no later than ten calendar days in advance of any proposed substitution and

SECTION H – SPECIAL CONTRACTS REQUIREMENTS

shall include justification (including resume(s) and labor category of proposed substitution(s)) in sufficient detail to permit evaluation of the impact on TO performance.

Substitute personnel qualifications shall meet the minimum requirements of a Project Manager listed in Section H.1.1. If the GSA CO and the GSA COR determine that a proposed substitute personnel is unacceptable, or that the reduction of effort would be so substantial as to impair the successful performance of the work under the TO, the contractor may be subject to default action in accordance with FAR 52.212-4, Contract Terms and Conditions Commercial items (May 2015) (Alternate I May 2014) (Deviation I Feb 2007) and GSAM 552.212-4 Contract Terms and Conditions Commercial Items (May 2015) (Alternate II Jul 2009) (FAR Deviations Jul 2015).

H.2 UNSATISFACTORY PERFORMANCE BY CONTRACTOR PERSONNEL

In the event that the performance of assigned Contractor personnel or any substitute(s) is determined by the Government to be unsatisfactory at any time during the life of the Task Order, the Government reserves the right to request and receive satisfactory personnel replacement within ten (10) calendar days of receipt by the Contractor of written notification. Notification will include the reason for requesting replacement personnel. Replacement personnel must have the same minimum qualifications and additional specialized or specific experience as the person replaced and meet the security requirements.

H.3 IDENTIFICATION OF CONTRACTOR EMPLOYEES

All Contractor/teaming partner/subcontractor personnel shall wear company picture identification badges as to distinguish themselves from Government employees when at the Government's site. When conversing with Government personnel during business meeting, over the telephone or via electronic mail, Contractor/teaming partner /subcontractor personnel shall identify themselves as such to avoid situations arising where sensitive topics might be better discussed solely between Government employees. Contractors/teaming partner/subcontractors shall identify themselves on any attendance sheet or any coordination documents they may review. Electronic mail signature blocks shall identify their company affiliation.

H.3 UNSATISFACTORY PERFORMANCE BY CONTRACTOR PERSONNEL

In the event that the performance of assigned Contractor personnel or any substitute(s) is determined by the Government to be unsatisfactory at any time during the life of the task order, the Government reserves the right to request and receive satisfactory personnel replacement within ten (10) calendar days of receipt by the Contractor of written notification. Notification will include the reason for requesting replacement personnel. Replacement personnel must have the same minimum qualifications and additional specialized or specific experience as the person replaced and meet the security requirements.

H.4 GOVERNMENT FURNISHED PROPERTY (GFP)

The Government shall provide office space, equipment and local telephone service for any on-site Contractor personnel, as appropriate. The Government shall provide system access for on-

SECTION H – SPECIAL CONTRACTS REQUIREMENTS

site and off-site work in accordance with agency standards, local security regulations and rules of conduct.

The Contractor shall ensure accurate control and accountability of all Government Furnished Property in accordance with terms and conditions of this task order. The Government will furnish, at no cost to the Contractor, the GFP shown below.

- Office space
- Laptops
- Necessary equipment for wired and wireless network connectivity
- DOC appropriate badging

H.5 GENERAL SUPPLIES AND EQUIPMENT

1. Contractor Provided Supplies and Equipment

The Contractor shall provide office supplies and materials required in the conduct of its own internal business.

2. Government Provided Supplies and Equipment

For contractor personnel located at the Herbert C. Hoover Building, the Government shall provide basic supplies and materials normally available to Government employees including personal computers and applications software.

H.6 INFORMATION TECHNOLOGY

Property furnished to the Contractor shall be in accordance with FAR Part 45. The Government will provide the Contractor with access to and use of information technology systems and components, which includes the following:

- Windows, Linux servers;
- Emergency Broadcast server;
- Servers for environmental monitoring;
- IP telephones (Cisco);
- Cisco switches and routers;
- Cisco network management software packages
- Network monitoring tools;
- Management laptops and supporting tools;
- Laboratory for staging and testing system version upgrades, configuration changes, etc.

The Government will supply the Contractor with personal computers and software necessary in the performance of this Task Order. All Government provided equipment will be maintained by the Government. The Contractor shall determine operational status of all equipment. It shall be

SECTION H – SPECIAL CONTRACTS REQUIREMENTS

the Contractor's responsibility to notify the COR or his designated representative of any malfunctions or suspected improper equipment performance.

H.7 GOVERNMENT FURNISHED INFORMATION (GFI)

The Government will provide the Contractor with access to information technology systems, documentation, and online resources (hardware and software vendors' technical documents and technical support resources) appropriate to their tasks. Individual Contractor staff's access and specific rights (e.g., root access) to systems is dependent on their job functions and the approval of DOC IT security staff.

H.8 SECURITY CONSIDERATIONS

H.8.1 KEY CONTROL

The Contractor shall ensure that all keys issued to contractor support personnel are accounted for and controlled. At a minimum, the Contractor shall be responsible for the following:

- 1) Ensuring keys are only used by the Contractor's employees.
- 2) Prohibiting the opening of locked areas by the Contractor's employees to permit entrance of persons other than the Contractor or DOC employees engaged in the performance of assigned work in those areas.
- 3) Ensuring keys issued to the Contractor by the Government are not duplicated.
- 4) Ensuring keys issued by the Government are not lost or misplaced.
- 5) Reporting the loss of any key in writing to the COR within eight (8) clock hours of occurrence or at the beginning of the next scheduled workday, whichever occurs first.
- 6) Reimbursing the Government to replace the lock if the Contractor lost the standard key. In the event the Contractor loses a master key, the Government will replace keys and all locks for that system, and the total cost shall be borne by the Contractor.

H.8.2 SECURITY CLEARANCES

At a minimum, one individual performing classified work under task 3 and one individual performing classified work under task 4 shall be cleared to a Top Secret clearance. These individuals will be the senior lead of the tasks and will require direct interaction with Enterprise Security Operations Center (ESOC) personnel. All personnel performing all other tasks must follow Department of Commerce's Security Manual for Public Trusts. Contractor's request for visit authorization when security access is required shall be submitted in accordance with Department of Defense (DOD) 5220.22M National Industrial Security Program Operating Manual (NISPOM) not later than one week prior to visit. A DD Form 254, Contract Security

SECTION H – SPECIAL CONTRACTS REQUIREMENTS

Classification Specification shall be coordinated with the Contractor and the program office at the time of the task order award. No classified work is authorized without an approved DD Form 254 and the appropriate personnel security clearances. Contractors must have valid personnel security clearances at the appropriate level at the time of contract award. If security requirements are not met or maintained, the Government reserves the right to terminate the contract.

Contractor's request for visit authorization shall be submitted in accordance with DOD 5220.22M (Industrial Security Manual for Safeguarding Classified Information) not later than one week prior to visit. Request shall be forwarded to the Department of Commerce, Office of Security, 1401 Constitution Ave, NW. Washington, DC 20230 Attn: Security Office, for certification of need to know by the specified GTR. All personnel performing classified tasks shall be cleared to a minimum of Top Secret. At the discretion of the GTR, Contractor personnel may begin the task with a Secret clearance that is in the process of being upgraded to a Top Secret security clearance with SCI eligibility.

H.8.3 PERSONNEL BACKGROUND INVESTIGATION REQUIREMENTS

The nature of the work performed under this SOW constitutes a High designation of risk as defined by [Commerce Acquisition Manual \(CAM\) 1337.70, Security Processing Requirements for Onsite Contracts](#). Therefore, all telecommunications tasks will be subject to the requirements of CAR 1352.237-70/1352.237-71 (text follows):

1352.237-70 SECURITY PROCESSING REQUIREMENTS – HIGH OR MODERATE RISK CONTRACTS

Security Processing Requirements—High or Moderate Risk Contracts (APR 2010)

(a) Investigative Requirements for High and Moderate Risk Contracts. All contractor (and subcontractor) personnel proposed to be employed under a High or Moderate Risk contract shall undergo security processing by the Department's Office of Security before being eligible to work on the premises of any Department of Commerce owned, leased, or controlled facility in the United States or overseas, or to obtain access to a Department of Commerce IT system. All Department of Commerce security processing pertinent to this contract will be conducted at no cost to the contractor. The level of contract risk will determine the type and scope of such processing, as noted below.

(1) Investigative requirements for Non-IT Service Contracts are:

- (i) High Risk—Background Investigation (BI).
- (ii) Moderate Risk—Moderate Background Investigation (MBI).

(2) Investigative requirements for IT Service Contracts are:

- (i) High Risk IT—Background Investigation (BI).

SECTION H – SPECIAL CONTRACTS REQUIREMENTS

(ii) Moderate Risk IT—Background Investigation (BI).

(b) In addition to the investigations noted above, non-U.S. citizens must have a pre-appointment check that includes an Immigration and Customs Enforcement agency check.

(c) Additional Requirements for Foreign Nationals (Non-U.S. Citizens). To be employed under this task order within the United States, non-U.S. citizens must have:

- (1) Official legal status in the United States;
- (2) Continuously resided in the United States for the last two years; and
- (3) Obtained advance approval from the servicing Security Officer of the contracting operating unit in consultation with the DOC Office of Security (OSY) headquarters. (OSY routinely consults with appropriate agencies regarding the use of non-U.S. citizens on contracts and can provide up-to-date information concerning this matter.)

(d) Security Processing Requirement. Processing requirements for High and Moderate Risk Contracts are as follows:

(1) The contractor must complete and submit the following forms to the Government's Technical Representative (GTR):

- (i) Standard Form 85P (SF-85P), Questionnaire for Public Trust Positions;
- (ii) FD-258, Fingerprint Chart with OPM's designation in the ORI Block; and
- (iii) Credit Release Authorization.

(2) The Sponsor will ensure that these forms have been properly completed, initiate the CD-254, Contract Security Classification Specification, and forward the documents to the cognizant Security Officer.

(3) Upon completion of security processing, the Office of Security, through the servicing Security Officer and the Sponsor, will notify the contractor in writing of an individual's eligibility to be provided access to a Department of Commerce facility or Department of Commerce IT system.

(4) Security processing shall consist of limited personal background inquiries pertaining to verification of name, physical description, marital status, present and former residences, education, employment history, criminal record, personal references, medical fitness, fingerprint classification, and other pertinent information. For non-U.S. citizens, the Sponsor must request an Immigration and Customs Enforcement agency check. It is the option of the Office of Security to repeat the security processing on any contract employee at its discretion.

(e) Notification of Disqualifying Information. If the Office of Security receives disqualifying information on a contract employee, the GTR/COR will be notified. The Sponsor, in coordination with the Contracting Officer, will immediately remove the contract employee from duties requiring access to Departmental facilities or IT systems. Contract employees may be barred from working on the premises of a facility for any of the following:

SECTION H – SPECIAL CONTRACTS REQUIREMENTS

- (1) Conviction of a felony crime of violence or of a misdemeanor involving moral turpitude;
- (2) Falsification of information entered on security screening forms or on other documents submitted to the Department;
- (3) Improper conduct once performing on the contract, including criminal, infamous, dishonest, immoral, or notoriously disgraceful conduct or other conduct prejudicial to the Government, regardless of whether the conduct was directly related to the contract;
- (4) Any behavior judged to pose a potential threat to Departmental information systems, personnel, property, or other assets.

(f) Failure to comply with security processing requirements may result in termination of the contract or removal of contract employees from Department of Commerce facilities or denial of access to IT systems.

(g) Access to National Security Information. Compliance with these requirements shall not be construed as providing a contract employee clearance to have access to national security information.

(h) The contractor shall include the substance of this clause, including this paragraph, in all subcontracts.

(End of clause)

1352.237-71 SECURITY PROCESSING REQUIREMENTS – LOW RISK CONTRACTS SECURITY PROCESSING REQUIREMENTS—LOW RISK CONTRACTS (APR 2010)

(a) Investigative Requirements for Low Risk Contracts. All contractor (and subcontractor) personnel proposed to be employed under a Low Risk contract shall undergo security processing by the Department's Office of Security before being eligible to work on the premises of any Department of Commerce owned, leased, or controlled facility in the United States or overseas, or to obtain access to a Department of Commerce IT system. All Department of Commerce security processing pertinent to this contract will be conducted at no cost to the contractor.

(b) Investigative requirements for Non-IT Service Contracts are:

- (1) Contracts more than 180 days—National Agency Check and Inquiries (NACI).
- (2) Contracts less than 180 days—Special Agency Check (SAC).

(c) Investigative requirements for IT Service Contracts are:

- (1) Contracts more than 180 days—National Agency Check and Inquiries (NACI).
- (2) Contracts less than 180 days—National Agency Check and Inquiries (NACI).

(d) In addition to the investigations noted above, non-U.S. citizens must have a background check that includes an Immigration and Customs Enforcement agency check.

SECTION H – SPECIAL CONTRACTS REQUIREMENTS

(e) Additional Requirements for Foreign Nationals (Non-U.S. Citizens). Non-U.S. citizens (lawful permanent residents) to be employed under this contract within the United States must have:

- (1) Official legal status in the United States;
- (2) Continuously resided in the United States for the last two years; and
- (3) Obtained advance approval from the servicing Security Officer in consultation with the Office of Security headquarters.

(f) DOC Security Processing Requirements for Low Risk Non-IT Service Contracts. Processing requirements for Low Risk non-IT Service Contracts are as follows:

- (1) Processing of a NACI is required for all contract employees employed in Low Risk non-IT service contracts for more than 180 days. The GTR will invite the prospective contractor into e-QIP to complete the SF-85. The contract employee must also complete fingerprinting.
- (2) Contract employees employed in Low Risk non-IT service contracts for less than 180 days require processing of Form OFI-86C Special Agreement Check (SAC), to be processed. The Sponsor will forward a completed Form OFI-86C, FD-258, Fingerprint Chart, and Credit Release Authorization to the servicing Security Officer, who will send the investigative packet to the Office of Personnel Management for processing.
- (3) Any contract employee with a favorable SAC who remains on the contract over 180 days will be required to have a NACI conducted to continue working on the job site.
- (4) For Low Risk non-IT service contracts, the scope of the SAC will include checks of the Security/Suitability Investigations Index (SII), other agency files (INVA), Defense Clearance Investigations Index (DCII), FBI Fingerprint (FBIF), and the FBI Information Management Division (FBIN).
- (5) In addition, for those individuals who are not U.S. citizens (lawful permanent residents), the Sponsor may request a Customs Enforcement SAC on Form OFI-86C, by checking Block #7, Item I. In Block 13, the Sponsor should enter the employee's Alien Registration Receipt Card number to aid in verification.
- (6) Copies of the appropriate forms can be obtained from the Sponsor or the Office of Security. Upon receipt of the required forms, the Sponsor will forward the forms to the servicing Security Officer. The Security Officer will process the forms and advise the Sponsor and the Contracting Officer whether the contract employee can commence work prior to completion of the suitability determination based on the type of work and risk to the facility (*i.e.* , adequate controls and restrictions are in place). The Sponsor will notify the contractor of favorable or unfavorable findings of the suitability determinations. The Contracting Officer will notify the contractor of an approved contract start date.

(g) Security Processing Requirements for Low Risk IT Service Contracts. Processing of a NACI is required for all contract employees employed under Low Risk IT service contracts.

- (1) Contract employees employed in all Low Risk IT service contracts will require a National Agency Check and Inquiries (NACI) to be processed. The GTR will invite the prospective contractor into e-QIP to complete the SF-85. Fingerprints and a Credit Release Authorization

SECTION H – SPECIAL CONTRACTS REQUIREMENTS

must be completed within three working days from start of work, and provided to the Servicing Security Officer, who will forward the investigative package to OPM.

(2) For Low Risk IT service contracts, individuals who are not U.S. citizens (lawful permanent residents) must undergo a NACI that includes an agency check conducted by the Immigration and Customs Enforcement Service. The Sponsor must request the ICE check as a part of the NAC.

(h) Notification of Disqualifying Information. If the Office of Security receives disqualifying information on a contract employee, the Sponsor and Contracting Officer will be notified. The Sponsor shall coordinate with the Contracting Officer for the immediate removal of the employee from duty requiring access to Departmental facilities or IT systems. Contract employees may be barred from working on the premises of a facility for any of the following reasons:

(1) Conviction of a felony crime of violence or of a misdemeanor involving moral turpitude.

(2) Falsification of information entered on security screening forms or of other documents submitted to the Department.

(3) Improper conduct once performing on the contract, including criminal, infamous, dishonest, immoral, or notoriously disgraceful conduct or other conduct prejudicial to the Government regardless of whether the conduct was directly related to the contract.

(4) Any behavior judged to pose a potential threat to Departmental information systems, personnel, property, or other assets.

(i) Failure to comply with security processing requirements may result in termination of the contract or removal of contract employees from Department of Commerce facilities or denial of access to IT systems.

(j) Access to National Security Information. Compliance with these requirements shall not be construed as providing a contract employee clearance to have access to national security information.

(k) The contractor shall include the substance of this clause, including this paragraph, in all subcontracts.

(End of clause)

H.9 CAR 1352.239-72 SECURITY REQUIREMENTS FOR INFORMATION TECHNOLOGY RESOURCES

Security Requirements for Information Technology Resources (APR 2010)

(a) *Applicability.* This clause is applicable to all contracts that require contractor electronic access to Department of Commerce sensitive non-national security or national security information contained in systems, or administrative control of systems by a contractor that process or store information that directly supports the mission of the Agency.

SECTION H – SPECIAL CONTRACTS REQUIREMENTS

(b) *Definitions.* For purposes of this clause, the term “Sensitive” is defined by the guidance set forth in the Computer Security Act of 1987 (Pub. L. 100–235), including the following definition of the term:

(1) Sensitive information is “ * * * any information, the loss, misuse, or unauthorized access to, or modification of which could adversely affect the national interest or the, conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (The Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy.”

(2) For purposes of this clause, the term “National Security” is defined by the guidance set forth in:

(i) The DOC IT Security Program Policy and Minimum Implementation Standards, Section 4.3.

(ii) The DOC Security Manual, Chapter 18.

(iii) Executive Order 12958, as amended, Classified National Security Information. Classified or national security information is information that has been specifically authorized to be protected from unauthorized disclosure in the interest of national defense or foreign policy under an Executive Order or Act of Congress.

(3) Information technology resources include, but are not limited to, hardware, application software, system software, and information (data). Information technology services include, but are not limited to, the management, operation (including input, processing, transmission, and output), maintenance, programming, and system administration of computer systems, networks, and telecommunications systems.

(c) The contractor shall be responsible for implementing sufficient Information Technology security, to reasonably prevent the compromise of DOC IT resources for all of the contractor's systems that are interconnected with a DOC network or DOC systems that are operated by the contractor.

(d) All contractor personnel performing under this contract and contractor equipment used to process or store DOC data, or to connect to DOC networks, must comply with the requirements contained in the DOC *Information Technology Management Handbook* (see DOC, Office of the Chief Information Officer Web site), or equivalent/more specific agency or operating unit counsel guidance as specified immediately hereafter [insert agency or operating unit counsel specific guidance, if applicable].

(e) Contractor personnel requiring a user account for access to systems operated by the contractor for DOC or interconnected to a DOC network to perform contract services shall be

SECTION H – SPECIAL CONTRACTS REQUIREMENTS

screened at an appropriate level in accordance with Commerce Acquisition Manual 1337.70, *Security Processing Requirements for Service Contracts*.

(f) Within 10 days after task order award, the contractor shall certify in writing to the GTR that its employees, in performance of the contract, have completed initial IT security orientation training on DOC IT Security policies, procedures, computer ethics, and best practices, in accordance with *DOC IT Security Program Policy*, chapter 15, section 15.3. The GTR will inform the contractor of any other available DOC training resources. Annually thereafter the contractor shall certify in writing to the GTR that its employees, in performance of the contract, have completed annual refresher training as required by section 15.4 of the *DOC IT Security Program Policy*.

(g) Within 10 days of task order award, the contractor shall provide the GTR with signed acknowledgement of the provisions as contained in Commerce Acquisition Regulation (CAR), 1352.209–72, *Restrictions Against Disclosures*.

(h) The contractor shall afford DOC, including the Office of Inspector General, access to the Contractor's and subcontractor's facilities, installations, operations, documentation, databases, and personnel used in performance of the contract. Access shall be provided to the extent required to carry out a program of IT inspection, investigation, and audit to safeguard against threats and hazards to the integrity, availability, and confidentiality of DOC data or to the function of computer systems operated on behalf of DOC, and to preserve evidence of computer crime.

(i) For all contractor-owned systems for which performance of the contract requires interconnection with a DOC network on which DOC data will be stored or processed, the contractor shall provide, implement, and maintain a System Accreditation Package in accordance with the *DOC IT Security Program Policy*. Specifically, the contractor shall:

(1) Within 14 days after task award, submit for DOC approval a System Certification Work Plan, including project management information (at a minimum the tasks, resources, and milestones) for the certification effort, in accordance with *DOC IT Security Program Policy* and [Insert agency or operating unit counsel specific guidance, if applicable]. The Certification Work Plan, approved by the GTR, in consultation with the DOC IT Security Officer, or Agency/operating unit counsel IT Security Manager/Officer, shall be incorporated as part of the task order and used by the COR/GTR to monitor performance of certification activities by the contractor of the system that will process DOC data or connect to DOC networks. Failure to submit and receive approval of the Certification Work Plan may result in termination of the task order.

(2) Within 14 days after approval, follow the work plan schedule to complete system certification activities in accordance with *DOC IT Security Program Policy* Section 6.2, and provide the GTR with the completed System Security Plan and Certification Documentation Package portions of the System Accreditation Package for approval and system accreditation by an appointed DOC official.

SECTION H – SPECIAL CONTRACTS REQUIREMENTS

(3) Upon receipt of the Security Assessment Report and Authorizing Official's written accreditation decision from the GTR, maintain the approved level of system security as documented in the Security Accreditation Package, and assist the GTR in annual assessments of control effectiveness in accordance with *DOC IT Security Program Policy*, Section 6.3.1.1.

(j) The contractor shall incorporate this clause in all subcontracts that meet the conditions in paragraph (a) of this clause.

(End of clause)

H.10 SAFETY

The Contractor shall:

1. Comply with all applicable safety and occupational health requirements, to include OSHA's 29 CFR 1910. If the Contractor fails or refuses to promptly comply with safety requirements, the Contracting Officer may issue an order stopping all or part of the work until satisfactory corrective action has been taken.

2. Verbally inform the GTR of any unsafe/hazardous conditions within thirty (30) minutes of becoming aware of the condition, and in writing within one (1) workday.

3. Verbally inform the GTR within two (2) clock hours of the occurrence of all types of injuries and illnesses (first aid, limited duty, lost time and fatality) sustained by a contractor employee arising out of and in the course of his/her employment; a detailed written report is required within 24 clock hours.

4. Report to the GTR all incidents where contractor employees damage government property. A verbal report shall be made within four (4) clock hours of an occurrence; a written report of the facts and extent of damage is due within three (3) workdays.

5. Take responsibility for all damages caused by negligence of its employees

H.11 FAR 52.228-5 INSURANCE--WORK ON A GOVERNMENT INSTALLATION.

Insurance--Work on a Government Installation (Jan 1997)

(a) The Contractor shall, at its own expense, provide and maintain during the entire performance of this contract, at least the kinds and minimum amounts of insurance required in the Alliant SB contract.

(b) Before commencing work under this contract, the Contractor shall notify the Contracting Officer in writing that the required insurance has been obtained. The policies evidencing required insurance shall contain an endorsement to the effect that any cancellation or any material change adversely affecting the Government's interest shall not be effective—

SECTION H – SPECIAL CONTRACTS REQUIREMENTS

- (1) For such period as the laws of the State in which this contract is to be performed prescribe; or,
 - (2) Until 30 days after the insurer or the Contractor gives written notice to the Contracting Officer, whichever period is longer.
- (c) The Contractor shall insert the substance of this clause, including this paragraph (c), in subcontracts under this contract that require work on a Government installation and shall require subcontractors to provide and maintain the insurance required in the Schedule or elsewhere in the contract. The Contractor shall maintain a copy of all subcontractors' proofs of required insurance, and shall make copies available to the Contracting Officer upon request.

H.12 FAR 52.228-7 INSURANCE--LIABILITY TO THIRD PERSONS.

Insurance--Work on a Government Installation (Mar 1996)

- (a)
- (1) Except as provided in subparagraph (a)(2) of this clause, the Contractor shall provide and maintain workers' compensation, employer's liability, comprehensive general liability (bodily injury), comprehensive automobile liability (bodily injury and property damage) insurance, and such other insurance as the Contracting Officer may require under this contract.
 - (3) The Contractor may, with the approval of the Contracting Officer, maintain a self-insurance program, provided that, with respect to workers' compensation, the Contractor is qualified pursuant to statutory authority.
 - (4) All insurance required by this paragraph shall be in a form and amount and for those periods as the Contracting Officer may require or approve and with insurers approved by the Contracting Officer.
- (b) The Contractor agrees to submit for the Contracting Officer's approval, to the extent and in the manner required by the Contracting Officer, any other insurance that is maintained by the Contractor in connection with the performance of this contract and for which the Contractor seeks reimbursement.
- (c) The Contractor shall be reimbursed—
- (1) For that portion—
 - (i) Of the reasonable cost of insurance allocable to this contract; and
 - (ii) Required or approved under this clause; and
 - (2) For certain liabilities (and expenses incidental to such liabilities) to third persons not compensated by insurance or otherwise without regard to and as an exception to the limitation of cost or the limitation of funds clause of this contract. These liabilities must arise out of the performance of this contract, whether or not caused by the negligence of the Contractor or of the Contractor's agents, servants, or employees, and must be

SECTION H – SPECIAL CONTRACTS REQUIREMENTS

represented by final judgments or settlements approved in writing by the Government. These liabilities are for—

- (i) Loss of or damage to property (other than property owned, occupied, or used by the Contractor, rented to the Contractor, or in the care, custody, or control of the Contractor); or
- (ii) Death or bodily injury.

(d) The Government's liability under paragraph (c) of this clause is subject to the availability of appropriated funds at the time a contingency occurs. Nothing in this contract shall be construed as implying that the Congress will, at a later date, appropriate funds sufficient to meet deficiencies.

(e) The Contractor shall not be reimbursed for liabilities (and expenses incidental to such liabilities)—

- (1) For which the Contractor is otherwise responsible under the express terms of any clause specified in the Schedule or elsewhere in the contract;
- (2) For which the Contractor has failed to insure or to maintain insurance as required by the Contracting Officer; or
- (3) That result from willful misconduct or lack of good faith on the part of any of the Contractor's directors, officers, managers, superintendents, or other representatives who have supervision or direction of—
 - (i) All or substantially all of the Contractor's business;
 - (ii) All or substantially all of the Contractor's operations at any one plant or separate location in which this contract is being performed; or
 - (iii) A separate and complete major industrial operation in connection with the performance of this contract.

(f) The provisions of paragraph (e) of this clause shall not restrict the right of the Contractor to be reimbursed for the cost of insurance maintained by the Contractor in connection with the performance of this contract, other than insurance required in accordance with this clause; *provided*, that such cost is allowable under the Allowable Cost and Payment clause of this contract.

(g) If any suit or action is filed or any claim is made against the Contractor, the cost and expense of which may be reimbursable to the Contractor under this contract, and the risk of which is then uninsured or is insured for less than the amount claimed, the Contractor shall—

- (1) Immediately notify the Contracting Officer and promptly furnish copies of all pertinent papers received;

SECTION H – SPECIAL CONTRACTS REQUIREMENTS

- (2) Authorize Government representatives to collaborate with counsel for the insurance carrier in settling or defending the claim when the amount of the liability claimed exceeds the amount of coverage; and
- (3) Authorize Government representatives to settle or defend the claim and to represent the Contractor in or to take charge of any litigation, if required by the Government, when the liability is not insured or covered by bond. The Contractor may, at its own expense, be associated with the Government representatives in any such claim or litigation.

H.13 FAR 52.237-2 PROTECTION OF GOVERNMENT BUILDINGS, EQUIPMENT, AND VEGETATION.

Protection of Government Buildings, Equipment, and Vegetation (Apr 1984)

The Contractor shall use reasonable care to avoid damaging existing buildings, equipment, and vegetation on the Government installation. If the Contractor's failure to use reasonable care causes damage to any of this property, the Contractor shall replace or repair the damage at no expense to the Government as the Contracting Officer directs. If the Contractor fails or refuses to make such repair or replacement, the Contractor shall be liable for the cost, which may be deducted from the contract price.

H.14 SPECIAL CONSIDERATIONS

1. The Contractor shall perform the tasks and provide documentation consistent with the guidelines in the following references and other pertinent Department of Commerce, OCIO, and government wide regulations:
 - a. Computer Security Act of 1987
 - b. Federal Information Security Management Act (FISMA)
 - c. OMB Circulars A-11, A-123, A-127, A-130
 - d. Homeland Security Presidential Directives 7 & 12
 - e. NIST's Special Publications 800-Series guidance documents
 - f. U.S. Government "Plain Language" Guidelines

2. Confidentiality *Corporate Non-Disclosure Agreement*

The Contractor may have to access proprietary information and shall be required to sign a (see Section J). The preliminary and final deliverables and all associated working papers, and other material deemed relevant by the agency that have been generated by the Contractor in the performance of this task order are the property of the U.S. Government and cannot be reproduced, or retained by the Contractor. When no longer required, this information, data, and/or equipment will be returned to Government control. All documents and information pertaining to network vulnerabilities, security policy, operational procedures or related functions shall be maintained under absolute accountability and relinquished to the OCIO GTR upon completion of the task.

SECTION H – SPECIAL CONTRACTS REQUIREMENTS

3. Task Order Special Instructions

All work performed under this task order must meet and comply with all National Institute of Standards & Technology (NIST), other government-wide laws and regulations, and Department of Commerce and OCIO directives, guidelines, and requirements for protection and security of Information Technology. Such directives and guidelines include but are not limited to:

GSA Order CIO 2100.1

4. Section 508 – Accessibility Compliance

Section 508 of the Rehabilitation Act requires Federal agencies to make their electronic and information technology accessible to people with disabilities. This applies to all Federal agencies when they develop, procure, maintain, or use electronic and information technology.

All electronic and information technology (EIT) procured through this contract must meet the applicable accessibility standards specified in 36CFR1194.2, unless an agency exception to this requirement exists. Any agency exceptions applicable to this contract are listed below.

The standards define Electronic and Information Technology, in part, as “any equipment or interconnected system or subsystem of equipment that is used in the creation, conversion, or duplication of data or information. The standards define the type of technology covered and set forth provisions that establish a minimum level of accessibility. The application section of the standards (1194.2) outlines the scope and coverage of the standards. The standards cover the full range of electronic and information technologies in the Federal sector, including those used for communication, duplication, computing, storage, presentation, control, transport and production. This includes computers, software, networks, peripherals and other types of electronic office equipment.

Applicable Standards, which apply to this acquisition

Section 1194.21: Software Applications and Operating Systems ____X____.
Section 1194.22: Web-based Internet Information and Applications ____X____.
Section 1194.23: Telecommunications Products ____X____.
Section 1194.25: Self-Contained, Closed Products ____X____.
Section 1194.26: Desktop and Portable Computers ____X____.
Section 1194.31: Functional Performance Criteria ____X____.

Agency Exceptions, which apply to this acquisition

National Security System _____.
Acquired by a contractor incidental to a contract _____.
Located in spaces frequented only by a service personnel for maintenance, repair or Occasional monitoring of equipment _____.
Would impose and undue burden on the agency _____.

SECTION H – SPECIAL CONTRACTS REQUIREMENTS

The Contractor shall ensure that all EIT products that are less than fully compliant are offered pursuant to extensive market research, which ensures that they are the most compliant products available to satisfy the solicitation's requirements.

If any such EIT product proposed is not fully compliant with all of the standards, the Contractor shall specify each specific standard that is not met; provide a detailed description as to how the EIT product does not comply with the identified standard(s); and shall also indicate the degree of compliance.

H.15 ORGANIZATIONAL CONFLICT OF INTEREST AND NON-DISCLOSURE REQUIREMENTS

The guidelines and procedures of FAR 9.5 will be used in identifying and resolving any issues of organizational conflict of interest at the Order level. FAR 3.104-4 will be utilized with regard to statutory and related prohibitions, restrictions, and requirements related to disclosing procurement information.

H.15.1 ORGANIZATIONAL CONFLICT OF INTEREST

If the contractor has or is currently providing support or anticipates providing support to DOC that creates or represents an actual or potential organizational conflict of interest (OCI), the contractor shall immediately disclose this actual or potential OCI in accordance with FAR Subpart 9.5. The contractor is also required to complete and sign an Organizational Conflict of Interest Statement in which the contractor (and any subcontractors, consultants, or teaming partners) agrees to disclose information concerning the actual or potential conflict with any proposal for any solicitation relating to any work in the TO. All actual or potential OCI situations shall be identified and addressed in accordance with FAR Subpart 9.5.

H.16 NON-DISCLOSURE REQUIREMENTS

All contractor personnel (to include subcontractors, teaming partners, and consultants) who will be personally and substantially involved in the performance of the task areas of this SOW which requires the contractor to act on behalf of, or provide advice with respect to any phase of an agency procurement, as defined in FAR 3.104-4, shall execute and submit a Non-Disclosure Agreement. This is required prior to the commencement of any work on such task and whenever replacement personnel are proposed under an on-going task.

H.17 ODCs

The Government may require the contractor to purchase supplies critical and related to the services being acquired under the contract. Such requirements will be identified during the course of a contract by the Government or the contractor. If the contractor initiates a purchase within the scope of this contract and the prime contractor has an approved purchasing system, the contractor shall submit to the AAS COR a Request to Initiate Purchase (RIP). If the prime contractor does not have an approved purchasing system at any point during contract performance, the contractor shall submit to the CO Consent to Purchase (CTP). The RIP and CTP shall include the purpose, specific items, estimated cost, cost comparison, and rationale.

SECTION H – SPECIAL CONTRACTS REQUIREMENTS

The contractor shall not make any purchases without an approved RIP from the COR or an approved CTP from the CO. The appropriate forms are attached in Section J.

H.18 TRAVEL

Contractor costs for travel will be reimbursed at the limits set in the following regulations (see FAR 31.205-46):

- a. Federal Travel Regulations (FTR) - prescribed by the GSA, for travel in the contiguous U.S.

H.18.1 TRAVEL AUTHORIZATION REQUEST

Before undertaking long distance travel to any site in performance of this TO, the contractor shall have this travel approved by, and coordinated with, the COR and the GTR. Notification shall include, at a minimum, the number of persons in the party, traveler name, destination, duration of stay, purpose, and estimated cost. Prior to any long distance travel, the contractor shall prepare a TAR for Government review and approval. Long-distance travel will be reimbursed for cost of travel comparable with the FTR and JTR.

Requests for travel approval shall:

- a. Identify the Contract number.
- b. Identify the CLIN associated with the travel.
- c. Contain the following:
 - i. Date, time and points of departure,
 - ii. Destination, time and dates of arrival,
 - iii. Name of each Contractor employee, company and position title traveling,
 - iv. Origin,
 - v. Dates of Travel,
 - vi. Organization to be visited,
 - vii. Purpose of Travel,
 - viii. Requesting Individual's Name,
 - ix. Estimate of Travel Funds Required (Include Airfare, Rental Car, Lodging, Transportation, Parking, POV mileage, Gasoline, Other),
 - x. GTR Concurrence
 - xi. COR Approval
- d. Be submitted in advance of the travel with 5 workdays to permit review and approval.

The contractor shall use only the minimum number of travelers and rental cars needed to accomplish the task(s). Travel shall be scheduled during normal duty hours whenever possible.

SECTION H – SPECIAL CONTRACTS REQUIREMENTS

H.19 TRANSFER OF HARDWARE/SOFTWARE MAINTENANCE AGREEMENTS

If the offeror proposes to provide any commercial computer software ("Commercial Software") as part of its proposed solution in response to this Solicitation, the offeror shall ensure that any software license agreement ("License Agreement") associated with such Commercial Software and intended to bind the Government complies with the FAR clause at 12.212(a), which provides, in relevant part, that commercial computer software and documentation shall be acquired under licenses customarily provided to the public "to the extent such licenses are consistent with Federal law." The most common examples of areas of non-compliance are set forth in the table below, which is provided for information purposes only and does not constitute an exhaustive list.

The requirement to propose compliant License Agreements shall apply regardless of whether the original rights holder to the Commercial Software ("Licensor") is the offeror, its subcontractor, or a third party, in the case of third-party software embedded or provided with the Commercial Software. Further, this requirement shall apply regardless of the format or title of the License Agreement, i.e., whether entitled "Software License Agreement," "End User License Agreement," "Terms of Service," or otherwise, and whether presented in hard copy or in a clickwrap or other electronic format. For the avoidance of doubt, this may require the offeror to negotiate with its Licensors and to obtain a revised version of the License Agreement. License Agreements incorporated into a company's existing Schedule 70 or other Government contract are not exempt from this requirement.

If proposing Commercial Software, the offeror shall include a statement in its proposal certifying that all applicable License Agreements will comply the requirement of this section H.25 (actual License Agreements need not be submitted prior to award). Failure to certify compliance will render the proposal ineligible for award, and non-compliance identified after award may entitle the Government to terminate the contract and seek any or all available remedies for breach of contract.

Commercial Terms*	Legal Restriction	Action**
Contract formation and modification	Under FAR 1.601(a), in an acquisition involving the use of appropriated funds, an agreement binding on the Government may only be entered into by a duly warranted contracting officer in writing. Under FAR 43.102, the same requirement applies to contract modifications affecting the rights of the parties.	Any provisions purporting to form a contract binding on the US Government by any other means (e.g., use, download, click through terms, etc.) must be deleted. The same applies to provisions allowing for License Agreement terms to be changed unilaterally by the Licensor.

<p>Patent or other type of intellectual property Indemnity – sellers of products or services often provide that in the event of claim or litigation alleging infringement of patent rights asserted by some third party that the seller will indemnify the buyer, provided that the buyer provide notice of the claim or litigation, and that the seller assume control of the litigation and any proposed settlement.</p>	<p>Under the authority of 28 USC § 516, only the Attorney General, acting by and through the attorneys of the US Department of Justice, may represent the US Government in litigation.</p>	<p>The patent or other type of intellectual property indemnity clause remains in effect, but any undertaking to "defend" the Government or any requirement that the seller control litigation and/or any proposed settlement is to be deleted.</p>
<p>General Indemnity – sellers of products or services provide that in the event of any litigation arising from the buyers use of the product or service that buyer will indemnify seller's litigation costs and damages (if any).</p>	<p>Agreements to pay the attorney fees of a private party require a statutory waiver of sovereign immunity. Agreements to pay some indeterminate amount of money in the future violate the restrictions of the Anti-Deficiency Act, 31 U.S.C. § 1341(a)(1) and the Adequacy of Appropriations Act, 41 USC §11.</p>	<p>General Indemnity clauses must be removed from the License Agreement.</p>
<p>Arbitration of disputes – sellers of products or services provide that any disputes with buyer must be resolved through binding arbitration without recourse to litigation in state or federal courts.</p>	<p>Federal Agencies are not allowed to use binding arbitration unless the head of the agency has promulgated guidance through administrative rulemaking on the use of binding arbitration. <i>See</i> 5 USC § 575. At the time of this Solicitation release, GSA has not done so.</p>	<p>Binding Arbitration clauses must be removed from the License Agreement.</p>
<p>Venue, Jurisdiction and Choice of Law – sellers of products or services provide that jurisdiction of any dispute will be in a particular state, federal or foreign court or that particular state or foreign law will govern.</p>	<p>Litigation where the US Government is a defendant must be heard either in US District Court (28 USC § 1346) or the US Court of Federal Claims (28 USC §1491). The US Government, as the sovereign, does not contract under state or foreign law. Depending on the subject matter of the dispute, the Contract</p>	<p>Clauses claiming that disputes will only be heard in state court will be revised to allow disputes in Federal court. Choice of law clauses must be deleted.</p>

	Disputes Act or other applicable law will govern.	
Equitable Remedies – sellers of products or services provide that in the event of a dispute concerning patent or copyright infringement that the end user agree that an injunction is appropriate.	The only remedy provided for copyright or patent infringement against the US Government is monetary damages. <i>See</i> 28 USC § 1498.	Equitable remedy clauses must be removed.
Negative Options – sellers of products or services provide that option periods will automatically be exercised unless affirmative action is taken by the buyer to not exercise the option.	Agreements to pay money in advance of appropriations violate the restrictions of the Anti-Deficiency Act, 31 U.S.C. § 1341(a) (1) and the Adequacy of Appropriations Act, 41 USC §11.	Negative option clauses must be removed.
Limitation of Liability	Various (see next column)	Limitation of liability clauses may be included in accordance with the Licensor's standard commercial practices, except that such clauses may not operate to impair or prejudice the U.S. Government's right (a) to recover for fraud or crimes arising out of or relating to this task order under any Federal fraud statute, including without limitation the False Claims Act (31 USC §§3729 through 3733), or (b) to express remedies provided under any FAR, DOCR or master Alliant contract clauses incorporated into this task order.
Integration/Order of Precedence Clauses		Any provisions purporting to invalidate or supersede the terms of the Government task order resulting from this Solicitation (such provisions are frequently found in "entire agreement" clauses) must be removed from the License Agreement.

SECTION H – SPECIAL CONTRACTS REQUIREMENTS

* The following standard commercial terms are deemed non-compliant within the meaning of this clause

** The License Agreement will be deemed compliant when the action specified in this column is successfully implemented

H.20 INTELLECTUAL PROPERTY RIGHTS

The existence of any patent, patent application or other intellectual property right that encumbers any deliverable must be disclosed in writing on the cover letter that accompanies the delivery. If no such disclosures are provided, "the data rights provisions in FAR 52.227-14 apply.

H.21 TELEWORK

Telework may be permissible, but all telework must have written approval by the GTR prior to telework. Telework arrangements on individual SOWs approval under the following:

Teleworking on the part of the company is voluntary.

1. Telework shall not result in an increase in task order price.
2. The Contractor is responsible for continuity of performance in accordance with the terms of the task order.
3. Company requests to telework shall be approved by the GTR
4. Any equipment provided by the Government for telework purposes will be treated as Government Furnished Equipment and guidelines in Controls for Government Property and Guidance on Removing Government Property from DOC Facilities shall be followed
5. Contractors shall provide a weekly telework report to the GTR prior to teleworking.

SECTION I – CONTRACT CLAUSES

I.1 FAR 52.252-2 CLAUSES INCORPORATED BY REFERENCE (FEB 1998)

This TO incorporates one or more clauses by reference with the same force and effect as if they were given in full text. Upon request, the GSA CO will make their full text available. Also, the full text of any provision is accessible electronically at: <https://www.acquisition.gov/far/>

Clause No	Clause Title	Date
52.222-60	Paycheck Transparency	(JAN 2016)
52.223-15	Energy Efficiency in Energy Consuming Products	(DEC 2007)
52.223-16	IEEE 1680 Standard for the Environmental Assessments of Personal Computer Products	(DEC 2007)
52.227-14	Rights in Data-General	(MAY 2014)
52.227-14	Rights in Data – General Alternative II	(DEC 2007)
52.227-15	Representation of Limited Rights Data and Restricted Computer Software	(DEC 2007)
52.228-5	Insurance-Work on a Government Installation	(JAN1997)
52.228-7	Insurance-Liability to Third Party Persons	(MAR 1996)
52.237-2	Protection of Government Buildings, Equipment and Vegetation	(APR 1984)
52.243-1	Changes-Fixed Price	(AUG 1987)
52.243-3	Changes-Labor Hours	(SEP 2000)

I.2 FAR CLAUSES IN FULL TEXT

I.2.1 FAR 52.217-8 OPTION TO EXTEND SERVICES (NOV 1999)

The Government may require continued performance of any services within the limits and at the rates specified in the contract. These rates may be adjusted only as a result of revisions to prevailing labor rates provided by the Secretary of Labor. The option provision may be exercised more than once, but the total extension of performance hereunder shall not exceed 6 months. The Contracting Officer may exercise the option by written notice to the Contractor within 15 days before expiration.

SECTION I – CONTRACT CLAUSES

(End of clause)

I.2.2 FAR 52.217-9 OPTION TO EXTEND THE TERM OF THE CONTRACT (MAR 2000)

(a) The Government may extend the term of this contract by written notice to the Contractor within 30 days before expiration, provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 15 days before the contract expires. The preliminary notice does not commit the Government to an extension.

(b) If the Government exercises this option, the extended contract shall be considered to include this option clause.

(c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed 60 months.

(End of clause)

I.2.3 FAR 52.237-3 CONTINUITY OF SERVICES (JAN 1991)

(a) The Contractor recognizes that the services under this contract are vital to the Government and must be continued without interruption and that, upon contract expiration, a successor, either the Government or another contractor, may continue them. The Contractor agrees to --

(1) Furnish phase-in training; and

(2) Exercise its best efforts and cooperation to effect an orderly and efficient transition to a successor.

(b) The Contractor shall, upon the Contracting Officer's written notice,

(1) Furnish phase-in, phase-out services for up to 90 days after this contract expires and

(2) Negotiate in good faith a plan with a successor to determine the nature and extent of phase-in, phase-out services required.

The plan shall specify a training program and a date for transferring responsibilities for each division of work described in the plan, and shall be subject to the Contracting Officer's approval. The Contractor shall provide sufficient experienced personnel during the phase-in, phase-out period to ensure that the services called for by this contract are maintained at the required level of proficiency.

(c) The Contractor shall allow as many personnel as practicable to remain on the job to help the successor maintain the continuity and consistency of the services required by this contract. The Contractor also shall disclose necessary personnel records and allow the successor to conduct on-site interviews with these employees. If selected employees are agreeable to the change, the Contractor shall release them at a mutually agreeable date and negotiate transfer of their earned fringe benefits to the successor.

(End of Clause)

SECTION I – CONTRACT CLAUSES

I.4 GENERAL SERVICES ADMINISTRATION ACQUISITION MANUAL (GSAM) CLAUSES INCORPORATED BY REFERENCE

The full text of a provision may be accessed electronically at: GSAM website:

<https://www.acquisition.gov/gsam/gsam.html>

Clause No	Clause Title	Date
552.212-4	Contract Terms and Conditions – Commercial Items (Alt II)	(JUL 2015)
552.232.25	Prompt Payment	(NOV 2009)
552.232-39	Unenforceability of Unauthorized Obligations	(JUL 2015)
552.232-78	Commercial Supplier Agreements-Unenforceable Clauses	(JUL 2015)

SECTION J – LIST OF ATTACHMENT

Attachment	Title
A	SF1449
B	Master SLA Document
C	IT Security Program Policies
D	Vulnerability Scanning and Patch Management
E	Change Control Board/Configuration Management
F	NOC and SOC Inventory
G	Key Personnel Qualification Matrix (To be removed at time of award)
H	Request to Initiate Purchase
I	Consent to Purchase
J	Corporate Non-Disclosure Agreement
K	Quality Assurance Surveillance Plan
L	Reading Room Instructions (To be removed at time of award)
M	Anticipated ODCs
N	Incidents by Priority
O	Incidents by Category
P	Incidents Resolved
Q	Requests by Category
R	ITSD 6 Month Tickets by Category
S	ITSD Call Abandonment Percentage
T	LAN Incidents by Month
U	Network Port Activation
V	SOC Incidents by Month
W	Security Configuration Checklist Program

**SECTION K – REPRESENTATIONS, CERTIFICATIONS, AND OTHER
STATEMENTS TO OFFEROR**

This page is intentionally left blank.

SECTION L – INSTRUCTIONS, CONDITIONS, AND NOTICE TO OFFERORS

L.1 52.252-1 SOLICITATION PROVISIONS INCORPORATED BY REFERENCE (FEB 1998)

This solicitation incorporates one or more solicitation provisions by reference, with the same force and effect as if they were given in full text. Upon request, the CO will make the full text available. The offeror is cautioned that the listed provisions may include blocks that must be completed by the offeror and submitted with its quotation or offer. In lieu of submitting the full text of those provisions, the offeror may identify the provision by paragraph identifier and provide the appropriate information with its quotation of offer. The solicitation provisions and/or contract clauses are available in either HTML or PDF format at:

<https://www.acquisition.gov/far>

<u>Clause No</u>	<u>Clause Title</u>	<u>Date</u>
52.232-38	Submission of Electronic Funds Transfer Information with Offer	(JUL 2013)

L.2 GENERAL INSTRUCTIONS

a. Offerors shall furnish the information required by this solicitation. A Standard Form (SF) 1449, "Solicitation/Contract/Order for Commercial Items" completed and signed by the offeror, Block 30, constitutes the offeror's acceptance of the terms and conditions of the proposed TOR. Therefore, the SF 1449 must be executed by a representative of the offeror authorized to commit the offeror to contractual obligations.

b. Offerors are expected to examine this entire solicitation document including the Contract. Failure to do so will be at the offeror's own risk.

c. The Government may make award based on initial offers received, without discussion of such offers. Proposals shall set forth full, accurate, and complete information as required by this solicitation package (including Attachments). The penalty for making false statements in proposals is prescribed in 18 U.S.C. 1001.

d. Offerors submitting restrictive data will mark it as follows: "Offerors who include in their proposals data they do not want disclosed to the public for any purpose or used by the Government except for evaluation purposes, shall:

Mark the title page with the following legend:

"This proposal includes data that shall not be disclosed outside the Government and shall not be duplicated, used or disclosed--in whole or in part--for any purpose other than to evaluate this proposal or quotation. If, however, a TO is awarded to this offeror as a result of/or in connection with the submission of this data, and the Government incorporates the proposal as part of the award, the Government shall have the right to duplicate, use, or disclose the data. Also, this

SECTION L – INSTRUCTIONS, CONDITIONS, AND NOTICE TO OFFERORS

restriction does not limit the Government's right to use information contained in this data if it is *obtained* from another source without restriction. The data subject to the restriction is contained in sheets (insert numbers or other identification of sheets)"; and

Mark each sheet of data it wishes to restrict with the following legend:

"Use or disclosure of data contained on this sheet is subject to the restriction on the title page of this proposal or quotation."

e. The Government assumes no liability for disclosure or use of unmarked data and may use or disclose the data for any purpose. Unless restricted, information submitted in response to this request may become subject to disclosure to the public pursuant to the provisions of the Freedom of Information Act (5 U.S.C. 551).

f. The authorized negotiator or the signatory of the SF 1449 will be notified of the date and time of the question and answer session. Offerors shall provide the name of the individual, the position title, telephone number, fax number, and electronic mail address of that individual.

g. This procurement is conducted under the procedures of FAR Subpart 16.5. The policies and procedures of FAR Subpart 15.3 do not apply.

h. The Government will not pay any offeror for preparation of their submission.

i. Offerors must submit their response by the date and time specified in the TOR. Late responses will be rejected and not considered for award.

j. Reading rooms located at DOC's headquarters will be made available to all contractors for the purpose of reviewing proprietary materials, guides, manuals, and documents pertinent to understanding the services and requirements under this procurement. (See Section J)

L.3 SUBMISSION OF QUESTIONS

Offerors are requested to submit questions grouped by solicitation section and make reference to the particular Section/Subsection number. Questions must be received before the date specified for receipt of questions. Questions or requests for extension submitted after the cut-off date will not be considered. Any questions regarding this solicitation shall be submitted no later than **April 25, 2017 at 3:00 PM Eastern Standard Time** via email to daniel.r.miller@gsa.gov and julius.bradshaw@gsa.gov. The information in response to questions concerning this solicitation will be furnished to offerors as an amendment to the solicitation.

L.4 GENERAL INFORMATION

Proposals will be valid for a period of 120 calendar days from the date of delivery.

SECTION L – INSTRUCTIONS, CONDITIONS, AND NOTICE TO OFFERORS

L.5 SUBMISSION OF PROPOSALS

All proposals shall be submitted electronically via ITSS, <https://portal.fas.gsa.gov>. All responses to the solicitation shall be received by 3:00 PM EST on Tuesday, May 9, 2017.

Each offer shall be in two parts. Part I is the written Cost/Price Proposal and shall contain the following:

- a. Solicitation, Offer and Award (SF 1449 (TAB A))
- b. Supplies or Services and Prices (TAB B)
- c. Price Supporting Documentation (TAB C)
- d. Organizational Conflict of Interest Statement (TAB D)
- e. Contract Registration (TAB E)
- f. ODCs Purchasing System (TAB F)

Part II is the written Technical Proposal and shall contain the following:

- a. Section 508 Compliance Statement. (Pass/Fail)
- b. Technical Approach
- c. Corporate Experience

L.6 SUBMISSION OF THE WRITTEN COST/PRICE PROPOSAL (PART 1)

The Written Price Proposal shall be submitted via email as prescribed above in Section L.5. The offeror shall submit all proposed prices using PDF, Microsoft Word or Excel software utilizing the formats without cells locked and include all formulas. There is no page limit on the written price proposal submission. The proposal shall contain the following tabs:

- a. Solicitation/Contract/Order for Commercial Items (SF 1449) (Tab A). When completed and signed by the Vendor constitutes the Vendor's acceptance of the terms and conditions of the proposed Contract. Therefore, the form must be executed by representatives of the Vendor authorized to commit the Vendor to contractual obligations. Vendors shall sign the SF 1449 in Block #30.
- b. Supplies or Services and Prices/Costs (Tab B). The Vendor shall indicate the price to be charged for each CLIN in Section B rounded to the nearest whole dollar.
- c. Price Supporting Documentation (Tab C). The information requested in the proposal is required to enable the Government to perform a price analysis. The contractor shall prepare one summary schedule which provides the total amount for each CLIN and the total price offered. Along with the summary schedule, the contractor is required to detail the labor categories to be used labor rates and labor hours proposed by category. The contractor shall also identify the discounts offered by the contractor.
- d. Organizational Conflict of Interest Statement (Tab D). The offeror shall provide an OCI Statement in which the offeror (and any subcontractors, consultants, or teaming partners) disclose information concerning actual or potential OCI affecting the offeror's proposal or any work related to this TOR. The statement should be accompanied by the offeror's plan for mitigation, avoidance, or neutralization, if appropriate.

SECTION L – INSTRUCTIONS, CONDITIONS, AND NOTICE TO OFFERORS

e. Contract Registration (Tab E). The offeror shall submit a statement that they are registered in ITSS (<https://portal.fas.gsa.gov>).

f. ODC Purchasing System (Tab F). The offeror shall submit a statement indicating if they possess a purchasing system approved by the Defense Contract Audit Agency or the cognizant audit agency and shall identify the organization that possesses that system and the audit agency that provided the approval.

NOTE: No Assumptions, Conditions, Exceptions are permitted. Any response containing Assumptions, Conditions, or Exceptions will be rejected and is ineligible for award.

L.7 SUBMISSION OF THE WRITTEN TECHNICAL PROPOSAL

The offeror shall submit all information described in the following paragraphs. The technical proposal must not exceed 25 double-sided sheets of paper, printed, exclusive of the cover page, table of contents, text and graphics, letters of commitment, resumes and staffing matrix. Text must be in a font equivalent to Times New Roman, Font 11, or larger. Tables may be no less than 10pt font and 8pt for graphics.

L.7.1 FACTOR 1 – SECTION 508 COMPLIANCE (PASS/FAIL)

The offeror's written proposal shall include a statement indicating its capability to comply with Section 508 requirements throughout its performance of this contract. The offeror's proposal will be evaluated to determine whether it includes a statement indicating its capability to comply with Section 508 requirements throughout its performance of this contract. Any proposal that does not include a statement indicating the offeror's capability to comply with Section 508 requirements throughout its performance of this contract shall be eliminated from further consideration for award.

L.7.2 FACTOR 2 - TECHNICAL APPROACH

The contractor shall identify and describe the methods and techniques to be used in fulfilling the technical requirements identified in the statement of work. The contractor should tailor the technical approach to achieve the requirements as identified in the solicitation. The technical approach shall clearly describe the following:

- a. The offeror's technical approach/solution for meeting the support services objectives in the task areas described in Section C of the TOR. The discussion shall identify the technical solution, to include the approach and methods for providing services for all tasks as described. The methodology shall clearly identify the technical approach and how it will address the goals, objectives, conditions, and task requirements.
- b. The offeror's knowledge of the core technologies mentioned in this TOR and the offeror's technical approach/solution for meeting the support services objectives and functional areas. The discussion shall identify the technical solution including the approach, methodology, analytical techniques and methodology.

SECTION L – INSTRUCTIONS, CONDITIONS, AND NOTICE TO OFFERORS

- c. The offeror shall submit a Key Personnel Qualification Matrix (Section J) for each Key Person proposed and the qualifications of the person or persons being proposed for that position. For those additional Key Personnel proposed, the offeror shall identify the specialized experience and the corresponding qualifications for this experience.

The offeror shall represent the following:

- All Key Personnel meet the requirements of the Alliant Small Business Contract.
- All Key Personnel meet the requirements of the TO under Section H, including security clearance requirements
- All Key Personnel named are available to begin work when the task order is awarded
- Letter of Commitment, signed by each proposed Key Person at the proposal submission due date.

*If additional Key Personnel are proposed by the offeror, the offeror shall specifically address the above for each.

These elements are not sub factors and will not be individually rated, but will be evaluated as a whole to arrive at the factor-level rating.

L.7.3 FACTOR 3 - CORPORATE EXPERIENCE

The Offeror shall provide a description of 3 contracts that are similar in scope and complexity performed (need not be completed) by the Prime Contractor or Proposed Key Subcontractor within the last 5 years. This can include contracts in support of the U.S. Government, state or local governments, commercial organizations, or other clients. Each corporate experience description shall not exceed three (3) pages in length.

The contractor shall provide the following information for each project example:

- a. Awarding Entity
- b. Program/project title
- c. TO/contract number that the work was performed under
- d. Contract amount per year and total amount
- e. Number of contractor personnel supporting the effort
- f. Description of the type of work performed
- g. Contractor's role – whether the work was performed as a prime/CTA member/subcontractor and the percentage and type of work performed by the contractor
- h. Period during which the work was performed (month/year for beginning and end) all years
- i. Contract type (FFP, T&M, CPFF, etc.)

SECTION L – INSTRUCTIONS, CONDITIONS, AND NOTICE TO OFFERORS

The Offeror (prime and/or proposed key subcontractor[s]) must possess recent Corporate Experience within the last 5 years with IT tier 0-3 service desk support; telecommunications and network support in a technical environment similar to the current DOC hardware, software, and network technologies; an environment that uses standard operating procedures; an environment that includes VOIP telephony; and an environment with at least 1,000 users and network nodes.

SECTION M – EVALUATION FACTORS FOR AWARD

M.1 METHOD OF AWARD

The Government anticipates awarding Task Orders to offerors whose proposal are the most advantageous to the Government, price and other factors considered. Technical proposals will be evaluated based on the factors described in Section L.7. All non-price evaluation factors, when combined, are significantly more important than price. Award may be made to other than the lowest priced, technically acceptable proposal.

M.2 EXPLANATION FOR BASIS OF AWARD

This acquisition is being conducted under FAR 16.5 principles and procedures of Subpart 15.3 do not apply. The Government may make award based on initial offers received, without discussion of such offers or the Government may make award after clarifications of some aspects of the proposal or discussions relative to price only. Accordingly, the Government reserves the right to do any or all of the following:

- Award on initial proposals, without discussion;
- Ask clarifying questions if needed. Clarification questions may include asking offerors to clarify statements made in the proposal. Clarification questions may include asking offerors to clarify their written technical proposals. As a result, the Government may have communications with some, but not all, offerors; these communications, however, will be clarifications and not discussions. In these situations, the Government will consider the offeror's clarifying response(s) without allowing proposal revisions;

M.3 PRICE PROPOSAL EVALUATION

The offeror's written price proposal will be evaluated by the Government for price reasonableness based on adequate price competition. Hourly labor rates proposed shall be at or below the Alliant Small Business GWAC awarded rates. The Government will reject any proposal that includes any assumptions, conditions or exception.

Tab D will be evaluated to assess whether or not an actual or potential Organizational Conflict of Interest exists as defined by FAR Part 9.5. If an actual or potential conflict of interest is identified that cannot be feasibly mitigated, avoided, or resolved in accordance with FAR Part 9.5, the offeror may be ineligible for award.

The government will evaluate the proposed number of labor hours and mix of labor in evaluating the total price as well as any discounts proposed. The contractor is requested to provide discounts from their Alliant Small Business contract pricing.

The Government will evaluate offers for award purposes by adding the total price for all options to the total price for the basic requirement. The Government may determine that a proposal is unacceptable if the option prices are significantly unbalanced. Evaluation of options shall not obligate the Government to exercise the option(s).

SECTION M – EVALUATION FACTORS FOR AWARD

For evaluation purposes, transition-out (CLIN 4001) is included in the last option period. However, the two month transition-out period will only occur once and may occur at the end of any performance period.

Any proposal received from a contractor not registered in ITSS (TAB E), will be rejected and will be ineligible for award.

NOTE: No Assumptions, Conditions, Exceptions are permitted. Any response containing Assumptions, Conditions, or Exceptions will be rejected and is ineligible for award.

M.4 OPTION TO EXTEND SERVICES (FAR 52.217-8)

The Government may require continued performance of any services within the limits and at the rates specified in the contract. These rates may be adjusted only as a result of revisions to prevailing labor rates provided by the Secretary of Labor. The option provision may be exercised more than once, but the total extension of performance hereunder shall not exceed 6 months. The Contracting Officer may exercise the option by written notice to the Contractor within 15 days before the contract expires.

To determine a total evaluated price, the Government will take the total price for the final option period, determine a six-month value, and add the value to the total amount proposed for all CLINS. Offerors shall **not** submit a price for the potential six-month extension of services.

M.5 TECHNICAL EVALUATION FACTORS

The Government will evaluate technical proposals based on the factors shown below. Section 508 Compliance will be evaluated on a pass/fail basis. A failure on any single Pass/Fail criteria will make the proposal ineligible for award, with no further evaluation of the technical and pricing proposal accomplished by the Government.

- a. Section 508 Compliance Statement (limited to one page). (Pass/Fail)
- b. Technical Approach
- c. Corporate Experience

The technical proposal evaluation factors are listed in descending order of importance. All 3 technical factors combined are significantly more important than cost. A failure on any single Pass/Fail criteria will make the proposal ineligible for award, with no further evaluation of the technical and pricing proposal accomplished by the Government.

M.5.1 FACTOR 1 – SECTION 508 COMPLIANCE (PASS/FAIL)

The offeror's proposal will be evaluated to determine whether it includes a statement indicating its capability to comply with Section 508 requirements throughout its performance of this Contract. Any proposal that does not include a statement indicating the offeror's capability to comply with Section 508 requirements throughout its performance of this Contract shall render the proposal ineligible for award, with no further evaluation of the technical and pricing proposal accomplished by the Government.

SECTION M – EVALUATION FACTORS FOR AWARD

M.5.2 FACTOR 2 - TECHNICAL APPROACH

The Government will evaluate the technical approach factor based on the clarity and completeness of the approach and the degree to which the proposal meets the requirements of the RFP (Section L.7.2).

Specifically, the Government will evaluate the technical approach based on the following:

- a. The quality, accuracy and completeness of the contractor's technical approach/solution for meeting the support services objectives in the areas described in Section C of the RFP. The discussion shall identify the technical solution, to include the approach and method for providing services for all tasks as described.
- b. The degree to which the contractor demonstrates the offeror's knowledge and understanding of the core technologies described in this TOR
- c. The degree of relevance of the stated qualifications, experience, skills, and roles of each of the named Key Personnel to meet the requirements of the TOR and support the offeror's technical approach.

M.5.3 FACTOR 3 – CORPORATE EXPERIENCE

The Government will evaluate the Corporate Experience factor based on the degree to which the offeror's:

- a. Corporate Experience reflects 3 contracts, performed within the last 5 years that are similar in scope and complexity to the requirements contained in Section C of the TOR.